(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 549 488 A1**

# (12) EUROPEAN PATENT APPLICATION

(21) Application number : **92420460.5**

(51) Int. Cl.[5] : **G11B 7/24**, G11B 7/26

(22) Date of filing : **14.12.92**

(30) Priority : **20.12.91 US 810976**

(43) Date of publication of application :
**30.06.93 Bulletin 93/26**

(84) Designated Contracting States :
**DE FR GB NL**

(71) Applicant : **EASTMAN KODAK COMPANY**
**343 State Street**
**Rochester, New York 14650-2201 (US)**

(72) Inventor : **Lentz, Joseph Paul, c/o EASTMAN KODAK COMPANY**
**Patent Legal Staff, 343 State Street**
**Rochester, New York 14650-2201 (US)**
Inventor : **Cushman, Thomas Richard, c/o EASTMAN KODAK COMPANY**
**Patent Legal Staff, 343 State Street**
**Rochester, New York 14650-2201 (US)**
Inventor : **Kline, Patrick Joseph, c/o EASTMAN KODAK COMPANY**
**Patent Legal Staff, 343 State Street**
**Rochester, New York 14650-2201 (US)**

(74) Representative : **Buff, Michel et al**
**Kodak-Pathé Département des Brevets et Licences CRT Centre de Recherches et de Technologie Zone Industrielle**
**F-71102 Chalon sur Saône Cédex (FR)**

## (54) A storage media for an optical information system having an identification code embedded therein.

(57) A optical storage disc for use in an optical storage system includes a storage layer which is capable of being disrupted when a laser beam of sufficient intensity is focused thereon. The optical storage disc has a transparent substrate layer on one side of the storage layer and a lacquer layer on the other side of the storage layer. The disruptions provided by the laser beam are selected to provide human readable and/or machine readable patterns. To reduce the damage to portions of the optical disc other than the storage layer, the storage layer is exposed to the laser beam prior to curing, or prior to applying and curing the lacquer layer. The optical disc can be of the type with data written thereon during fabrication, or the disc can be of the type in which data can be impressed thereon after fabrication of the optical disc. The patterns on the optical disc can be in the form of optical bar codes. In one application of the present invention involving the type of disc on which data can be written after fabrication, the pattern resulting from application of the laser beam to the disc is read by an optical reading device and transferred to the disc in the data format.

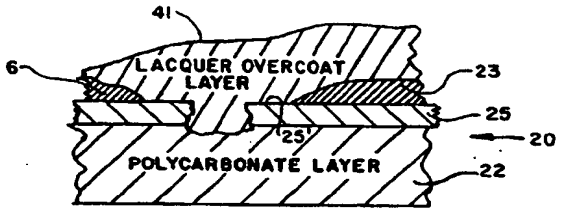



FIG. 4B

EP 0 549 488 A1

## BACKGROUND OF THE INVENTION

### 1. Field of Invention

This invention relates generally to the media upon which information is stored in an optical information storage and retrieval unit and, more particularly, to the inclusion in the media of an indelible identifying code.

### 2. Description of the Related Art

At the present state of technology, the optical storage disc is the preferred medium for read-only storage of large quantities of information. In this medium, the information is retrieved through the interaction of a radiation beam with the storage medium. At present, three principal types of optical storage discs are in common use. The first type of optical storage disc is manufactured with the information stored therein, generally in the form depressions formed into a polycarbonate substrate. A reflecting coating is deposited on the polycarbonate substrate and the radiation beam is focused on the reflecting layer. This type of optical disc is frequently referred to as a CD audio disc or a ROM (i.e., read only memory) disc. The second type of optical storage disc has the capability of having information recorded (written) thereon at some time after the fabrication of the disc. Such an optical storage disc is frequently referred to as a writable optical storage disc. The third type of optical storage disc has the capacity to have information recorded on the disc after fabrication. In addition, at a later time the stored information can be erased or modified. This type of optical storage disc is generally referred to as an erasable or a re-writable optical storage disc. In each type of optical storage disc, the storage layer is supported and protected by a polycarbonate support substrate and by a protective (lacquer) overcoat layer. However, the storage layer is modified in the writable disc and in the erasable disc. The storage layer in the writable disc includes a reflector layer (generally fabricated from gold) proximate the lacquer overcoat layer and includes a recording layer, typically a dye polymer layer, proximate the polycarbonate layer. The newly fabricated writable optical storage disc has a recording layer that is responsive to radiation having selected parameters, the radiation changing the optical properties of the recording layer. Differences in the optical properties of the recording layer can be detected, through the interaction with an impinging radiation beam and information, encoded by means of the optical property changes, can be recovered. In order to simplify the discussion, the recording, storage, and/or the reflective layer of the writable optical disc will be referred to as the storage layer.

During and after the manufacturing process, a need has been felt for a technique for providing permanent identification for the disc. In this manner, any problems that might originate with the manufacturing process can be related to discs fabricated during the same period of time or even to the same batch. Similarly, the history of the usage of the disc can be determined when a record is kept of the identifying information at the time of the accessing of the disc.

In the prior art, information has been applied to the surface of the disc, by means of mechanical disruption of the surface or by deposition of legible material on the surface. This information, however, being on the surface of the disc can be compromised either accidentally or intentionally.

Recently, in U.S. Patent No. 4,961,077 issued to D. L. Wilson et al., a technique for the permanent labelling of the discs was described. Specifically, the metal reflective layer, upon which the permanent identification information is stored as areas of varying reflectivity, is marked by means of a pulsed laser. The pulsed laser causes an indelible marking on the reflective layer, a marking which is protected by the same transparent coating which protects the reflective coating. The process described in the Wilson reference is extremely sensitive to the energy level of the laser beam, too small an energy level in the laser beam not providing an identifiable marking, while too much energy can disrupt the lacquer overcoat layer and/or the polycarbonate layer used to protect the reflective layer. The disruption of the storage layer can result in damage to the surrounding portions of the optical disc. In addition, applying the laser beam to the reflective surface through the narrower of the two protective coatings is recommended to minimize the destructive effects of the laser beam resulting from the passage of high intensity radiation through the layers.

A need has been felt for a technique for providing indelible identifying markings for the discs storing optical information which is relatively insensitive to the power of the radiation beam and which reduces the damage to the optical disc. Also needed is a technique for enhancing the machine readability of the disc markings.

## SUMMARY OF THE INVENTION

The present invention is directed to overcoming one or more of the problems set forth above. Briefly summarized, according to one aspect of the present invention, the marking of the disc is performed on the storage layer of the optical disc, however, the marking is performed prior to the curing of the protective lacquer overcoat or prior to the application of the protective overcoat itself. Because the lacquer overcoat, prior to curing of this material, is relatively elastic, the disruption of the overcoat as a result of the laser interaction with the reflective layer can be accomplish-

ed without excessive damage. The markings provided by the laser beam are arranged in preselected patterns, the patterns including machine readable and human readable information. According to one embodiment, optical bar code patterns can be printed in a manner that the position of an optical bar code reader relative to the center of the disc is irrelevant in interpreting the optical bar code message.

These and other aspects, objects, features and advantages of the present invention will be more clearly understood and appreciated from a review of the following detailed description of the preferred embodiments and appended claims, and be reference to the accompanying drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a cross sectional view of an optical storage disc of the type generally referred to as a read-only optical storage disc.

Figure 2 is a cross sectional view of an optical disc of the type generally referred to as a writable optical storage disc.

Figure 3A illustrates a first embodiment of a process by which machine readable and human readable information can be indelibly fixed in the optical storage media, and Figure 3B illustrates a.second embodiment of a process by which machine readable and human readable information can be indelibly fixed in an optical storage media.

Figure 4 is a cross sectional view of a mark in an optical storage disc generated as a result of the process illustrated in Figure 3A, while Figure 4B is a cross sectional view of a mark in an optical storage disc generated as a result of the process illustrated in Figure 4B.

Figure 5 illustrates an optical disc having machine readable and human readable text printed thereon.

Figure 6 illustrates how the optical bar code characters are formed according to the present invention.

Figure 7 is a block diagram of the storage medium and the read/write head including apparatus associated therewith of the storage and retrieval unit.

## DESCRIPTION OF THE PREFERRED EMBODIMENTS

### 1. Detailed Description of the Figures

Referring to Figure 1, a cross-sectional view of a read-only optical storage disc 10 for storing prerecorded data (in a form which can be identified by a radiation beam interacting with the disc) is shown. Transparent polycarbonate or substrate layer 12, or similar material has an optical transmission characteristic which permits the radiation interacting with the storage layer structure of the optical disc to be transmitted therethrough. The polycarbonate layer also acts as a support and protection layer for the remainder of the optical disc. Next to the polycarbonate layer 12 is the aluminum reflector layer 11. The polycarbonate layer 12 is fabricated with the stored information as a surface structure. The reflecting layer is deposited in such a manner as to provide a surface generally retaining the structure of the polycarbonate surface. A lacquer or other protective overcoat layer 13 is applied to the aluminum reflector layer in an uncured state. The lacquer or protective layer is typically of the type which is cured by ultraviolet radiation and the cured lacquer layer 13 supports and protects the aluminum reflector layer 11. In the past, identification markings 14 have been typically printed on the surface of the lacquer overcoat layer 13 or mechanically scribed in the surface of lacquer overcoat layer 13.

Referring to Figure 2, a writable optical storage disc 20 used for the storage of information is shown. In this type of optical storage disc, the data can be 'written' on the disc after the disc is fabricated. As with the optical storage disc of Figure 1, the writable optical disc includes a polycarbonate substrate of support layer 22. The storage layer 5 of the disc consists of a recording layer 21, which can be a dye polymer layer, and reflector layer 25, which can be fabricated from gold. Next to the reflector layer 25 is a lacquer overcoat layer 23, which is applied and then cured. Finally, the markings 24 on the surface of the disc provide human and machine readable information.

Referring to Figure 3A, the process for providing indelible information on a disc is shown. In step 31, the several layers of the optical disc is assembled. In step 32, the storage layer and the reflecting layer of the optical disc has information applied thereto, typically by using laser radiation to disrupt an interior surface region. In step 33, the lacquer overcoat layer is cured, providing the final step in the fabrication of an optical disc according to the present invention. In Figure 3B, an alternative process for providing indelible information on an optical disc is shown. In step 35, several layers of the optical disc are assembled. However, the surface region of the storage layer and reflective layer, on which the writing is to be inscribed, does not have the lacquer or protective coating applied thereon. In step 36, the marking of the surface is accomplished. In the preferred embodiment, this marking is accomplished by focused high intensity radiation, such as focused laser radiation. In step 37, the newly applied protective overcoat is applied to the region which has been marked and, if required, the protective coating is cured.

Referring to Figure 4A, a phenomenalogical representation of an identifying mark on an optical disc, capable of having information written thereon after fabrication, is shown. The disc 20 is fabricated with a polycarbonate layer 22, a reflecting layer 25, and a lacquer overcoat layer 23. The disruption 4 caused by

the laser radiation is in the reflector layer 25, depending on the intensity of the radiation can extend to or into the polycarbonate layer. In Fig. 4B, the disc 20 is assembled with the polycarbonate layer 22, the reflecting layer 25, and the lacquer or protective overcoat layer 23. However, a region 25' is not covered by the lacquer overcoat. The radiation causes a disruption in a selected region of the reflecting layer 25. The radiation parameters can be adjusted to provide relatively little impact on the polycarbonate substrate. The region without the lacquer overcoat can have also have printing applied thereto. The additional lacquer overcoat is applied, protecting the disrupted and/or printed region and protecting the information represented thereby from compromise.

Referring to Figure 5, a top view of a optical storage disc, particularly a type of disc 50 known as a compact disc (CD) is shown. The optical disc 50 typically has four regions which, with increasing radius can be defined as the following. Aperture 56 provides a structure to engage a spindle for controlled rotation of the disc. The next area is a clamp area 53. The clamp area 53 typically does not have a storage layer associated therewith and is used to provide a space wherein the spindle can be mechanically coupled to the disc without interfering with access to the data stored on the disc. The mirror area 52 has a storage layer associated therewith but does not have data embedded therein and, therefore, has a mirror-like appearance. Data area 51 of disc 50 has data stored on the storage layer including the reflecting layer associated therewith and, consequently, because of the structure in the reflecting layer, has a dull appearance when compared to the mirror-like appearance of mirror area 52. The mirror area 52 can be labelled in either a machine readable code 55 and/or with human readable markings by the process described in Figure 3A and Figure 3B, and illustrated by Figure 4A and Figure 4B. The disc 50 can therefore be labelled or marked by carbonizing the plastic in clamp area 53, marking the mirror area 52 of an optical disc 50 in the presence of an uncured lacquer overcoat layer 23 and then curing the lacquer overcoat layer as described above, marking the mirror area 52 of the disc prior to application of the protective overcoat 41 and curing of the lacquer overcoat region 41 after application of the protective coating, or marking the mirror region 52 after the protective layer 23 is cured. In the preferred embodiment, a group of alpha/numeric characters 57 are printed in the clamp area 53 and identifying fabrication information. Alpha/numeric characters 58 are provided in a human readable format and are printed on the surface of the mirror region 52. Code characters 59 are provided in the mirror region 52 in a machine readable (i.e., bar code) format.

Referring to Figure 6, an expanded view of the technique for writing information capable of being interpreted by an optical bar code reader in a manner in which the distance of the reader from the center of the disc is not important, even though the linear velocity of the optical code past the reader is a function of radius. The optical bar code markings 61 are formed by marking the area between two radius lines 61 and 62 from a first radial distance ($R_1$) 64 to a second radial distance ($R_2$) 65. With this bar code configuration, for a constant angular velocity of the disc, the distance of a bar code reader from the center of the disc is irrelevant. The time each bar interacts optically with the detector of the optical bar code reader retrieving information from the storage is independent of the distance from the disc center.

Referring to Figure 7, apparatus for reading the machine readable markings on an optical disc 70 is shown. A read/write head 75 applies radiation suitable for reading information to the markings to the disc. The reflected radiation has an intensity modulated by the identification markings 72. The optical read/write head 75 can identify the intensity of the reflected signal, or, the detector 76 can identify transmitted radiation. The resulting signals from either read/write head 75 or from detector 76 are applied to the analyzing and storage apparatus 77 where the data is processed and, when required stored. When the optical disc 70 is a disc upon which information can be written, the analyzing and storage apparatus 77 can be used to control the information written on the disc. In this manner, the information identifying the optical disc can be encoded and written on the data portion of the disc in a format compatible with the other data written thereon.

Briefly summarized, according to one aspect of the present invention, the marking of the disc is performed on the storage layer of an optical storage disc, however, the marking is performed prior to the curing of the lacquer overcoat layer according to one embodiment and prior to the application of the lacquer coating in a second embodiment. In the optical storage disc of the present invention, the overcoat is fabricated from a lacquer material for which ultraviolet light provides the curing reaction and reduces the elasticity of the overcoat.

## 2. Operation of the Preferred Embodiment

The purpose of the invention is to provide a technique for the application of an indelible identifying marks to an optical disc. Briefly summarized, according to one aspect of the present invention, the marking of the disc is performed on the storage layer, however, the marking is performed prior to the curing of, or prior to the application of the lacquer or protective overcoat layer. Where not previously applied, the protective overcoat is then applied. The lacquer material is then exposed to ultraviolet light which provides the curing for the lacquer overcoat layer. By marking storage layer prior to curing of the lacquer overcoat layer,

the lacquer overcoat layer, when present remains pliable enough to absorb damage that would otherwise result from the disruption of the polycarbonate layer.

In the optical disc capable of having information written or stored thereon after fabrication, the present invention has an important application. A facility capable of only reading the optical disc would typically not have the apparatus to interpret the optical bar code. Without the ability of read and interpret the bar code automatically, information can be stored on the disc which is not appropriate for that disc. Therefore, at the facility where the data is added to the fabricated disc, an optical bar code reader can be used to identify the optical bar code information and to include the information automatically in the data written or stored on the disc. In other words, the simultaneous presence of bar coded encoded information and equivalent information stored in the format of the information written on the optical disc insures that the disc has not been compromised.

While the storage medium has been described both in general terms and in terms of an optical disc, other medium for the storage of optical information, which have the general layer structure of the optical disc, can use the present invention advantageously. In addition, the storage layer has been described as generally including a reflective layer. The use of the reflection of radiation from a storage disc is generally used to identify the information stored thereon. However, the use of an optical storage disc which relies on the interaction of transmitted radiation with the storage media could use the present invention advantageously.

Similarly, while the invention has been described with particular reference to a preferred embodiment, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted for elements of the preferred embodiment without departing from invention. In addition, many modifications may be made to adapt a particular situation and material to a teaching of the invention without departing from the essential teachings of the present invention. By way of specific example, the lacquer layer used proximate the storage layer could be implemented with any material having properties suitable for the protection of the storage layer. By way of a different example, in the erasable optical disc, the storage layer can be selected of a material wherein an impinging radiation beam this appropriate parameters can provide a non-reversible change can take place. The non-reversible change protected from compromise by the protective overcoat layer.

As is evident from the foregoing description, certain aspects of the invention are not limited to the particular details of the examples illustrated, and it is therefore contemplated that other modifications and applications will occur to those skilled in the art. It is accordingly intended that the claims shall cover all such modifications and applications as do not depart from the true spirit and scope of the invention.

## Claims

1. A optical storage disc capable of having identifiable marking stored thereon, said markings resulting from an interaction of a laser beam with said optical storage disc, said optical storage disc comprising:

   a support substrate layer, said support substrate layer being transparent;

   a storage layer proximate said support substrate layer and capable of having data stored thereon, said storage layer having a preselected pattern of disruptions in a selected region resulting from irradiation by said laser beam;

   a protective layer covering said proximate said storage layer.

2. The optical storage disc of Claim 1 wherein said protective layer is applied prior to fabrication of said preselected pattern of disruptions, said protective layer being cured after fabrication of said preselected pattern of disruptions.

3. The optical storage disc of Claim 1 wherein said protective layer is applied to said selected region after fabrication of said preselected pattern of disruptions.

4. The optical storage disc of Claim 3 wherein said pattern of disruptions in said storage layer can be human readable or machine readable.

5. The optical disc of Claim 3 wherein said pattern of disruptions can be read by an optical bar code reader.

6. The optical storage disc of Claim 5 wherein said pattern of disruptions is structured such that a position of said optical bar code reader with respect to said field is independent of radial position.

7. The optical storage disc of Claim 3 wherein said storage disc is selected from the group of optical discs comprised of write-once optical discs, writable optical discs and erasable optical discs data identified by said pattern of disruptions being written on a mirror region of said optical disc.

8. The optical storage disc of Claim 3 wherein said storage layer includes a dye polymer layer.

9. The optical storage disc of Claim 1 wherein said pattern of disruptions includes information with

respect to the fabrication of said disc.

10. A method of permanently marking an optical storage disc, said method comprising the steps of:
assembling an optical disc having a storage layer and a polycarbonate layer;
applying a pattern of disruptions on a selected region of said storage layer with a laser beam; and
protecting said selected region of said storage layer with a lacquer layer.

11. The method of Claim 10 wherein said optical disc can be a write-once optical disc or a writable optical disc, a writable optical disc having a recording layer associated with said reflecting layer.

12. The method of Claim 11 wherein said protecting step includes a step of covering said selected region with a lacquer overcoat prior to said applying step and curing said lacquer overcoat after said applying step.

13. The method of Claim 11 wherein said protecting step includes a step of covering said selected region with a protective overcoat following said applying step.

14. The method of Claim 13 further comprising a step of selecting said pattern of disruptions to provide an optical bar code, wherein a thickness of each bar code character is a linear function of distance from a center of said optical disc.

15. The method of Claim 13 further comprising the steps of:
during a write operation for a writable or erasable optical disc, reading by a optical bar code reader said pattern of disruptions, and
writing information identified by said optical bar code reader in a data format on said writable or erasable optical disc.

16. An optical disc of a type having a polycarbonate substrate layer and a storage layer, said storage layer having a pattern of disruptions providing identifying markings, wherein the improvement is characterized by:
protecting said pattern of disruptions in a selected region by a protective layer consisting of a material requiring a curing operation, wherein said protective layer is cured after providing said identifying markings.

17. The optical disc of Claim 16 wherein said protective layer requires a curing operation, said optical disc further characterized by applying said protective layer to said selected region prior to providing said identifying markings.

18. The optical disc of Claim 16 further characterized by applying said protective overcoat to said selected region after providing said identifying markings.

19. The optical disc of Claim 18 further characterized by selecting said pattern of disruptions to represent data in bar code format.

20. The optical disc of Claim 18 wherein said optical storage disc is a writable optical storage disc having a recording layer associated with said storage layer, said optical storage disc further characterized by said data in bar code format replicated on said recording layer in an storage layer format.

21. The optical storage disc of Claim 18 further characterized by optical bar code characters positioned to be read by scanning the characters during rotation of the disc, said optical bar code characters having an angular width that is a linear function of radial position.

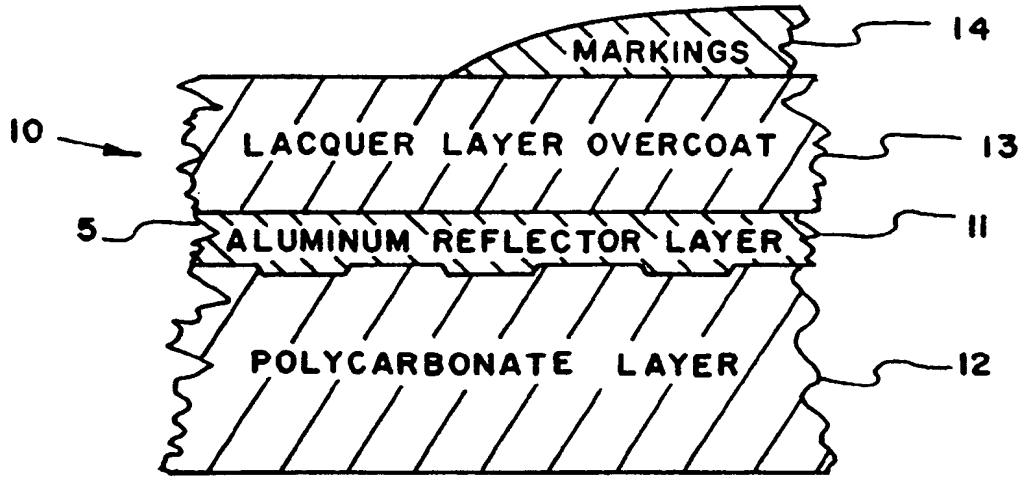

MARKINGS
14
10
LACQUER LAYER OVERCOAT
13
5
ALUMINUM REFLECTOR LAYER
11
POLYCARBONATE LAYER
12

FIG. 1

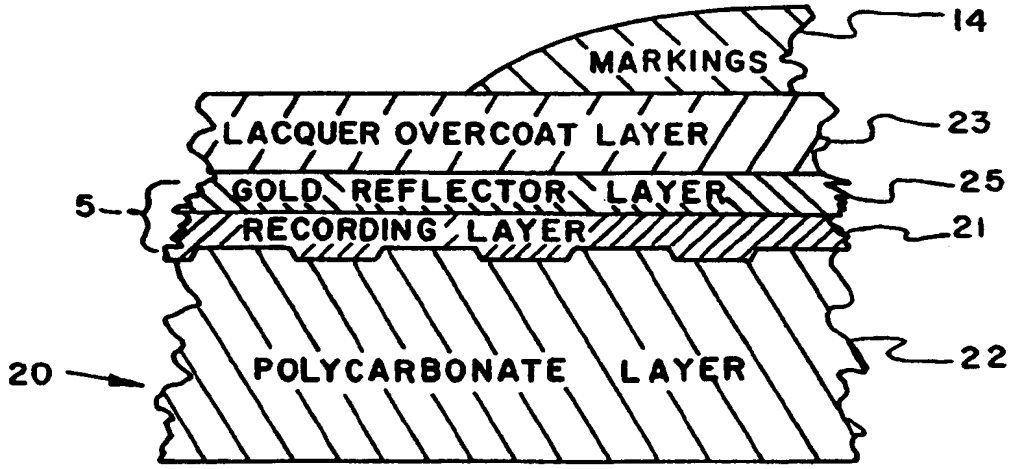

MARKINGS
14
LACQUER OVERCOAT LAYER
23
5
GOLD REFLECTOR LAYER
25
RECORDING LAYER
21
20
POLYCARBONATE LAYER
22

FIG. 2

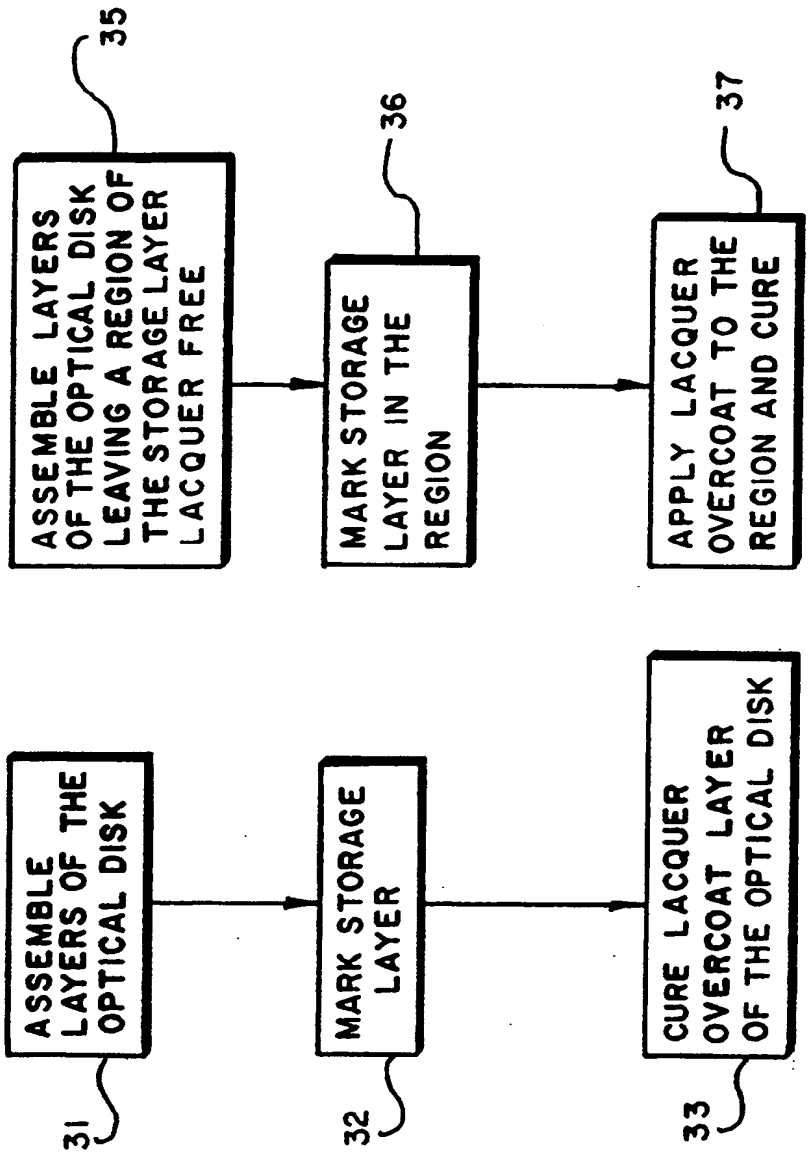

ASSEMBLE LAYERS OF THE OPTICAL DISK
31
MARK STORAGE LAYER
32
CURE LACQUER OVERCOAT LAYER OF THE OPTICAL DISK
33
ASSEMBLE LAYERS OF THE OPTICAL DISK LEAVING A REGION OF THE STORAGE LAYER LACQUER FREE
35
MARK STORAGE LAYER IN THE REGION
36
APPLY LACQUER OVERCOAT TO THE REGION AND CURE
37

FIG. 3A

FIG. 3B

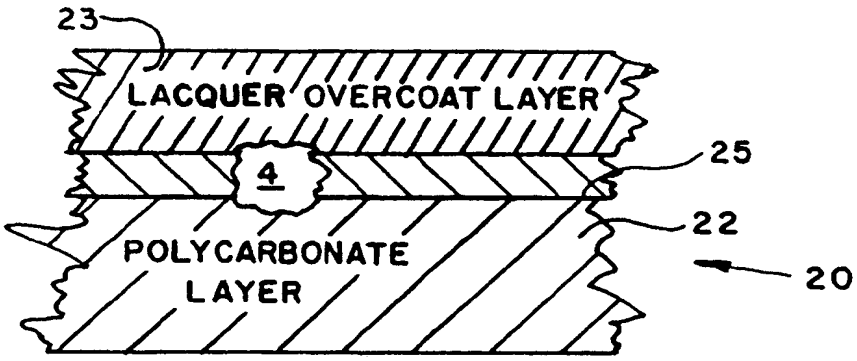

23
LACQUER OVERCOAT LAYER
25
4
22
POLYCARBONATE LAYER
20

FIG. 4A

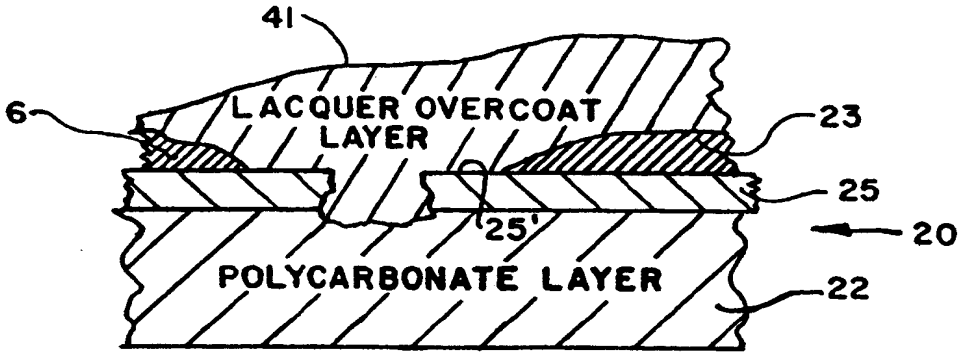

41
6
LACQUER OVERCOAT LAYER
23
25
25'
20
POLYCARBONATE LAYER
22

FIG. 4B

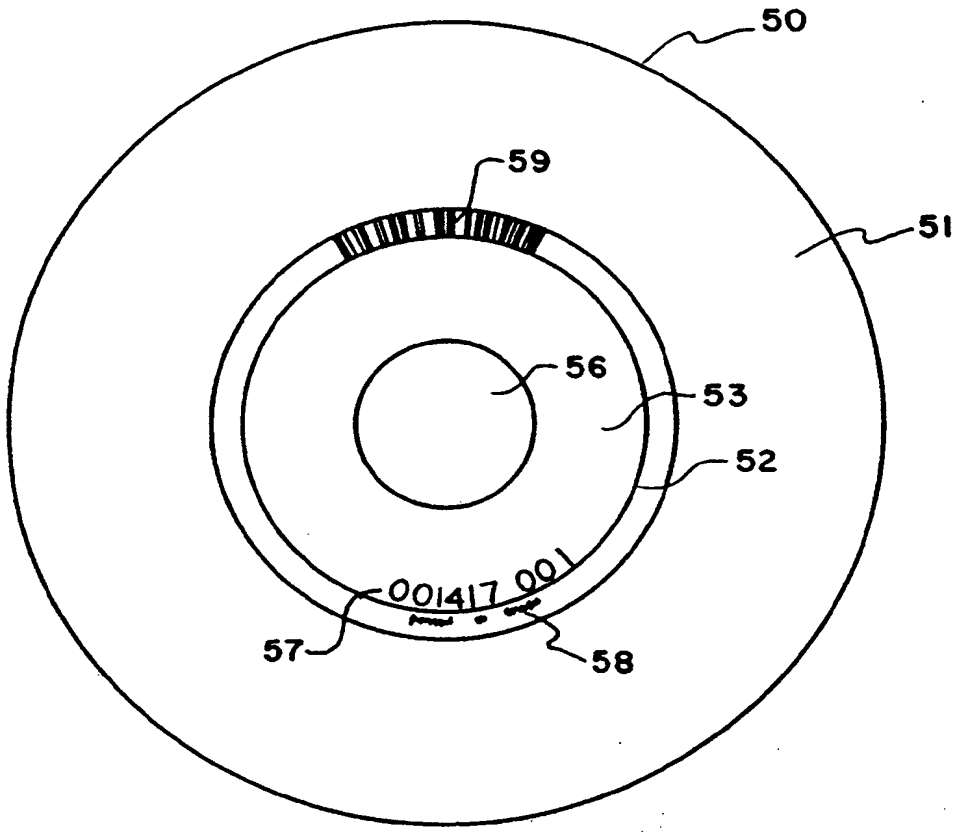



FIG. 5

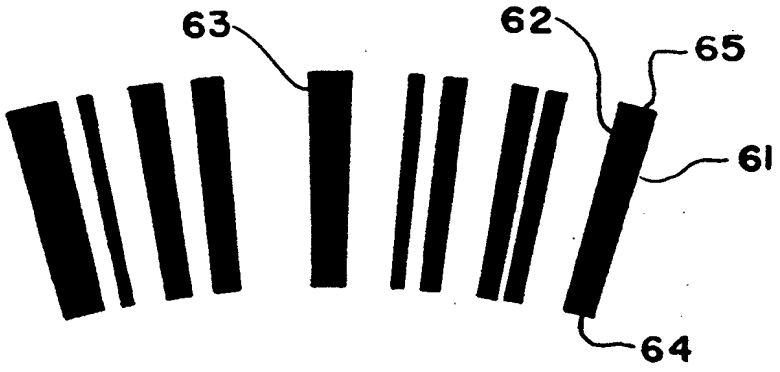



FIG. 6

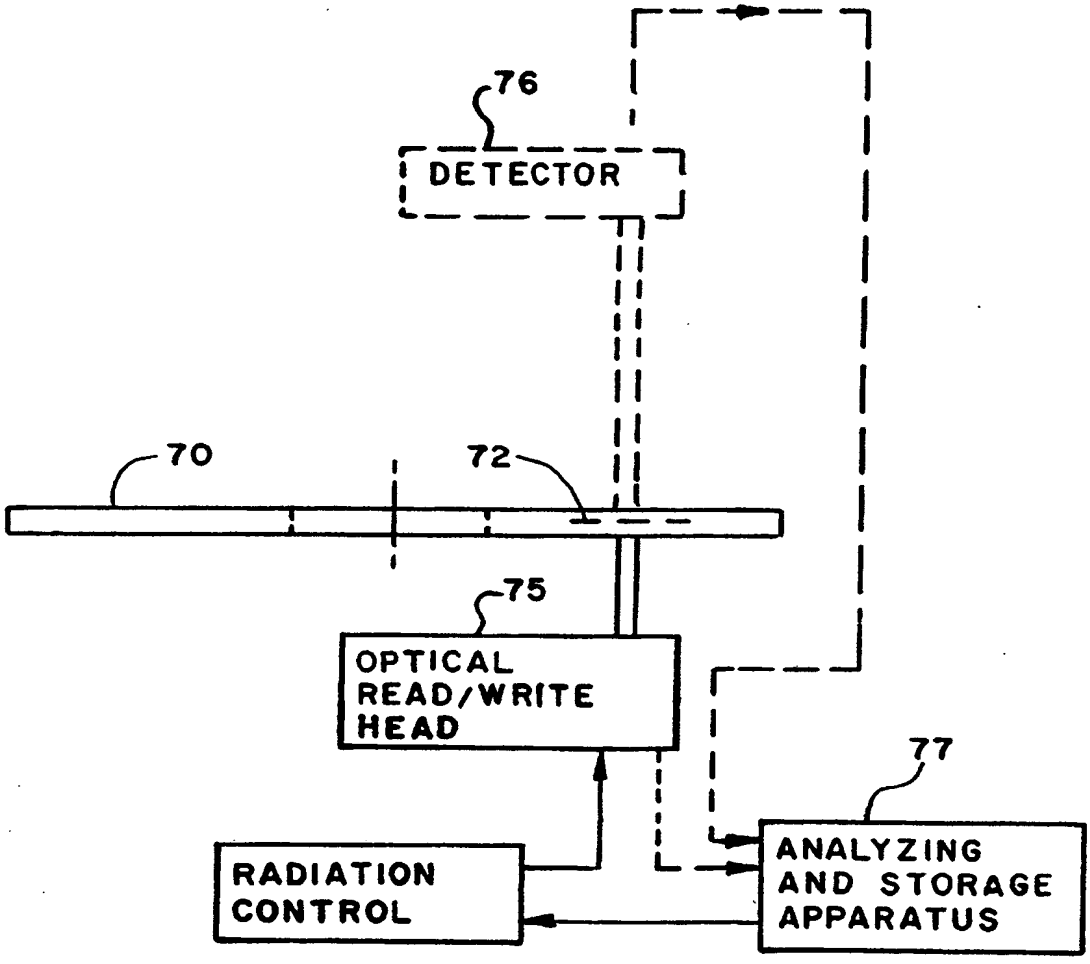

76
DETECTOR
70
72
75
OPTICAL
READ/WRITE
HEAD
77
RADIATION
CONTROL
ANALYZING
AND STORAGE
APPARATUS

FIG. 7

European Patent Office

# EUROPEAN SEARCH REPORT

Application Number EP 92420460.5

## DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (Int. Cl.5) |
|---|---|---|---|
| X | US - A - 4 805 046 (KUROKI et al.) * Fig. 1; column 1, lines 9-40; abstract; claim 1 * | 1,10 | G 11 B 7/24<br>G 11 B 7/26 |
| A | | 2-9, 11-21 | |
| A | EP - A - 0 225 259 (ALCATEL THOMSON GIGADISC) * Abstract * | 1-21 | |
| A | EP - A - 0 329 122 (PHILIPS AND DU PONT OPTICAL COMPANY) * Fig. 1-3; abstract * | 1-21 | |

TECHNICAL FIELDS SEARCHED (Int. Cl.5)

G 11 B 7/00
G 11 B 5/00

The present search report has been drawn up for all claims

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| VIENNA | 24-02-1993 | BERGER |

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 802 527 A1

# (12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
**22.10.1997 Bulletin 1997/43**

(21) Application number: **96932845.9**

(22) Date of filing: **08.10.1996**

(51) Int. Cl.[6]: **G11B 7/00**, G11B 20/10, G06F 12/14, G06F 9/06

(86) International application number:
**PCT/JP96/02924**

(87) International publication number:
**WO 97/14144 (17.04.1997 Gazette 1997/17)**

(84) Designated Contracting States:
**DE FR GB**

(30) Priority: **09.10.1995 JP 261247/95**
**23.01.1996 JP 8910/96**
**09.08.1996 JP 211304/96**

(71) Applicant:
**MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.**
**Kadoma-shi, Osaka-fu, 571 (JP)**

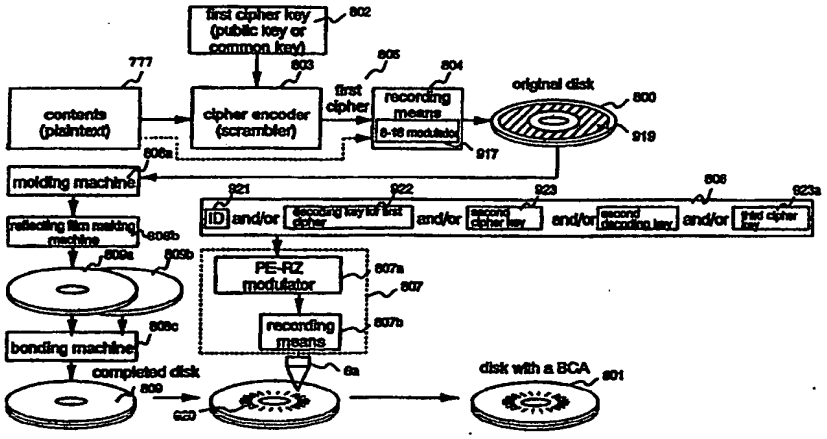
(72) Inventors:
- **OSHIMA, Mitsuaki**
  **Kyoto-shi Kyoto 615 (JP)**
- **GOTOH, Yoshiho**
  **Osaka 536 (JP)**
- **TANAKA, Shinichi**
  **Kyoto 610-03 (JP)**
- **KOISHI, Kenji**
  **Sanda-shi Hyougo 669-13 (JP)**
- **MORIYA, Mitsurou**
  **Nara 630-01 (JP)**
- **TAKEMURA, Yoshinari**
  **Osaka 566 (JP)**

(74) Representative: **Kügele, Bernhard et al**
**NOVAPAT INTERNATIONAL SA,**
**9, Rue du Valais**
**1202 Genève (CH)**

## (54) OPTICAL DISK, OPTICAL RECORDER, OPTICAL REPRODUCING DEVICE, ENCRYPTED COMMUNICATION SYSTEM, AND AUTHORIZING SYSTEM FOR USE OF PROGRAM

(57) The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures are simplified.

Fig. 1




EP 0 802 527 A1

## Description

### TECHNICAL FIELD

The present invention relates to an optical disk, an optical disk system and a cryptocommunication method.

### BACKGROUND

In recent years, with the increased use of networks such as the Internet and optical CD ROM disks, network soft key distribution for optical ROM disks has increased. Also, electronic commercial transactions have increased.

Soft key electronic distribution systems for CD-ROM media have been used. In conventional systems, it is known to give passwords and decipher the enciphered soft ciphers recorded on the CD-ROMs in advance. When CD-ROMs are used, however, it is not possible additionally to record on the disks, so that it is not possible to individually set IDs for respective disks. Therefore, one password would release the ciphers of all the disks manufactured from the same original disk. For this reason, when CD-ROMs are used, it is necessary to install the disks' IDs on the hard disks of personal computers, or mail to users IDs prepared centrally.

In electronic distribution systems with conventional optical disks and/or optical disk systems, there is a need to provide the disks and/or systems with IDs and/or cipher keys. It is an object of the present invention to simply provide IDs and cipher keys for ROM disks in electronic distribution systems.

### SUMMARY OF THE INVENTION

To achieve the objects of the present invention, the pit portions of optical disks are provided with an additional recording area or Burst Cutting Area (hereinafter abbreviated as BCA) overwritten with a bar code and, when the disks are manufactured, IDs differing for each disk and, according to the need, cipher keys for communication and decoding keys for decoding key cipher texts for communication, are recorded individually in the BCA areas. As a result, when the disks have been distributed to users, the user ID numbers, the cipher keys for transmission for communication, and the decoding keys for reception are distributed automatically to the users. It is therefore possible to omit some of the procedures that complicate conventional systems. Also, cryptocommunication and the identification of disks are made possible at the same time.

### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a flow chart of an optical disk according to an embodiment of the present invention.

Figs. 2a-c are cross sections and results of trimming with a pulse laser according to an embodiment of the invention.

Figs. 3a-g show the signal reproduction waveforms at a trimming portion according to an embodiment of the invention.

Fig. 4 is a block diagram of a reproducer according to an embodiment of the invention.

Fig. 5a shows the waveform of a reproduced signal at a BCA part according to the invention. Fig. 5b shows dimensional relationships of a BCA part according to the invention.

Fig. 6 shows a method of cryptocommunication and a cipher key method by means of a password according to an embodiment of the present invention.

Figs. 7a-c show the format of a BCA according to the invention.

Fig. 8 shows a method of cryptocommunication and a method of unlocking a cipher with a password according to an embodiment of the invention.

Fig. 9 shows a procedure for operation of a disk, the content part of which may have been licensed, according to an embodiment of the invention.

Fig. 10 is a block diagram of an example wherein a BCA has been recorded in a RAM disk according to an embodiment of the present invention.

Fig. 11 is a block diagram of a method or system for prevention of unauthorized copying according to an embodiment of the invention.

Fig. 12 is a flow chart depicting preventing unauthorized copying according to an embodiment of the invention.

Fig. 13a is a plan view and Fig. 13b is a cross section of an optical disk, on the BCA of which an article or commodity bar code has been printed, according to an embodiment of the invention. Fig. 13c shows a method of producing an optical disk according to an embodiment of the invention.

Fig. 14 is a block diagram of a POS settlement system with a ROM disk having a BCA and a POS terminal according to an embodiment of the invention.

Fig. 15 is a flow chart of cipher release in and between a press company, a software company and a selling store, according to an embodiment of the present invention.

Figs. 16 and 17 are flow charts (Parts 1 and 2, respectively) of steps of enciphering and decoding cipher data with a disk ID and/or the like according to an embodiment of the invention.

Figs. 18, 19 and 20 are flow charts (Parts 1, 2 and 3, respectively) of communication cipher key distribution and cryptocommunication with a BCA according to an embodiment of the invention.

Figs. 21, 22 and 23 are flow charts (Parts 1, 2 and 3, respectively) of an electronic settlement system with a BCA according to an embodiment of the present invention.

Fig. 24 is a block diagram of a method of recording and reproducing for recording limitation to one RAM disk with a BCA according to an embodiment of the

invention.

At the end of this specification is appended a list identifying items corresponding to the reference numerals used in the aforementioned drawings, that listing being in consecutive numerical order of the reference numerals.

## DETAILED DESCRIPTION OF THE INVENTION

The present invention will be described on the basis a number of embodiments. Herein, an additional recording area using the BCA system is referred to as a 'BCA area', and data recorded in a BCA is referred to as 'BCA data'. In addition, first identification data is referred to as 'ID' or 'disk ID'.

Fig. 1 shows a typical process for producing a disk with a BCA. The first cipher key 802, such as a public key, is used by a cipher encoder or scrambler 803 to encipher contents 777 into the first cipher 805. An 8-16 modulator 917, such as a mastering unit, modulates the first cipher 805. A laser records the modulated signal as pits in the first recording area 919 of an original disk 800. A molding machine 808a uses the original disk 800 to mold disk-like transparent substrates (not shown). A reflecting film making machine 808b forms reflecting Al films, and makes single-sided disks 809a and 809b which are each 0.6 millimeter thick. A bonding machine 808c laminates these disks together to make a completed disk 809. A trimming unit 807 modulates the disk ID 921, the first cipher decoding key 922, or the second cipher key 923 for Internet communication in the second recording area 920 of the completed disk 809, with a Phase Encoding-Return to Zero (PE-RZ) modulator 807a, which combines PE modulation and RZ modulation. A pulse laser 807b effects BCA trimming to make a disk 801 with a BCA. Because laminated disks are used, it is not possible to alter the BCA inside, and thus the completed disk can be used for security.

A BCA will next be explained briefly.

As shown in Fig. 2a, a pulse laser 808 trims the reflecting aluminum films 809 of the two-layer disk 800 in a BCA to record a stripe-like low reflection part 810 on the basis of a PE modulating signal. As shown in Fig. 2b, BCA stripes are formed on the disk. If the stripes are reproduced by a conventional optical head, the BCA has no reflecting signal. Therefore, as shown in Fig. 2c, gaps 810a, 810b and 810c are produced, where the modulating signal is missing. The modulating signal is sliced at the first slice level 915. But, the gaps 810a-c have a low signal level, and can therefore be sliced easily at the second slice level 916. As shown with the recorded and reproduced waveforms in Fig. 3, it is possible to reproduce the formed bar codes 923a and 923b by level-slicing them at the second slice level 916 by a conventional optical pickup as shown in Fig. 3e. As shown in Fig. 3f, the waveforms of the codes are shaped by a LPF filter so as to PE-RZ decode the codes. As shown in Fig. 3g, a digital signal is output.

With reference to Fig. 4, the decoding operation will be explained. A disk 801 with a BCA includes two transparent substrates, which are laminated with a recording layer 801a between them. The recording layer may either be a single layer 801a or include two recording layers 800a and 800b. If there are two layers, a BCA flag 922 is recorded in the control data of the first recording layer 800a, which is adjacent to the optical head 6. The flag 922 indicates whether a BCA is recorded or not. Because a BCA is recorded in the second layer 800b, the first recording layer 800a is focused on first, and the optical head 6 is moved to the radial position of the control data 924 in the innermost edge of the second recording area 919. The control data is main data, and has therefore been Eight to Fourteen Modulation (EFM), 8-15 or 8-16 modulated. Only when the BCA flag 922 in the control data is '1', a single/double layer switching part 827 focuses on the second recording layer 801b to reproduce the BCA. If the signal is sliced by a level slicer 590 at the general first slice level 915 as shown in Fig. 2c, it is converted into a digital signal. This signal is demodulated in the first demodulation part by an EFM demodulator 925, an 8-15 modulator-demodulator 926 or an 8-16 modulator-demodulator 927. An ECC decoder 36 corrects errors, if any, and outputs main data. The control data in the main data is reproduced and only if the BCA flag 922 is 1 is the BCA read. When the BCA flag 922 is 1, a CPU 923 orders the single/double layer switching part 827 to drive a focus adjustment part 828, switching the focus from the first recording layer 801a to the second recording layer 801b. At the same time, the optical head 6 is moved to the radial position of the second recording area 920, that is, for the DVD standard, the BCA is recorded between 22.3 and 23.5 mm from the inner edge of the control data. Then the BCA is read. Reproduced in the BCA area is a signal with a partially missing envelope as shown in Fig. 2c. By setting in the second level slicer 929 the second slice level 916 of which the quantity of light is smaller than that of the first slice level 915, it is possible to detect the missing parts of the reflecting portion of the BCA, and a digital signal is output. This signal is PE-RZ demodulated by the second demodulation part 930, and ECC decoded by an ECC decoder 930b so as to output BCA data, which is auxiliary data. Thus, the first demodulator 928, operative according to, 8-16 modulation demodulates and reproduces the main data, while the second demodulation part 930 operative according to PE-RZ modulation demodulates and reproduces the auxiliary data, that is, the BCA data.

Fig. 5a shows the reproduced waveform before passage through a filter 943. Fig. 5b shows the working size accuracy (precision) of the slits of the low reflecting portion 810. It is difficult to make the slit width less than 5mm. In addition, if the data is not recorded inward radially from 23.5 mm, it will not be properly reproduced. Therefore, for a DVD, because of the limitations of the shortest recording cycle of 30 mm and the maximum radius of 23.5 mm, the maximum capacity after formatting is limited to 188 bytes or less.

The modulating signal is recorded as pits by the 8-16 modulation mode, and a high frequency signal such as the high frequency signal part 933 in Fig. 5a is obtained. However, the BCA signal is a low frequency signal like low frequency signal part 932. Thus, if the main data complies with the DVD standard, it is a high frequency signal 932 which is about 4.5 MHz or less, shown in Fig. 5a, and the auxiliary data is a low frequency signal 933 which is 8.92 ms in period, that is, about 100 kHz. It is therefore relatively simple to frequency-separate the auxiliary data with a LPF 943. A frequency-separating method 934 as shown in Fig. 4, including the LPF 943 can easily separate the two signals. In this case, the LPF 943, may be simple in structure.

The foregoing is an outline of the BCA.

With reference to Fig. 6, the overall system of a cipher software unlatching system, narrowed down to the operations of password issue, cryptocommunication, and orderer certification, will be described. The steps in a press factory are nearly the same as in Fig. 1, so the original disk 800 and the completed disk 809 are not shown.

In a press factory 811, a cipher encoder 812 enciphers the data in the plaintexts 810 of the first to the '1-m'th contents or scrambles the picture signals therein with the first to '1- m'th cipher keys 813, respectively. The data or the signals are then recorded on an original optical disk 800. Disk-like substrates 809 are pressed from the original disk 800. After a reflecting film is formed on each substrate 809, the two disk-like substrates are laminated together. Thereafter a completed disk 809 is made. Recorded in the BCA areas 814 of completed disks 809 are different IDs 815 and/or first cipher keys 816 (public keys) and/or second cipher keys 817 (public keys) and second computer connection addresses 818 so as to make disks 801 each with a BCA. The disks 801 are distributed to users.

The contents of these disks have been enciphered. Therefore, in order to reproduce the contents of each of the disks, it is necessary to get a password from a password issue center, an electronic shop or a mall, by paying a charge. That procedure will be described next.

In a user's first computer 909, if a reproducer 819 reproduces a distributed disk 801 with a BCA, a BCA reproduction part 820 including a PE-RZ demodulation part reproduces the data of the ID 815, first cipher key 816, second cipher key 817 and/or connection address 818. In order to get a password, the connection address 818 of the second computer 821a, which is the server of a password issue center 821, is accessed through a communication part 822 via the Internet or another network 823, and the ID is transmitted to the second computer 821a.

Here, the cryptocommunication procedure will be described. The second computer 821a receives the ID 815 from the user's reproducer 819. Then, the second computer or server 821a of the password issue center 821, which is called a 'mall' or an 'electronic shop' has a cipher key database 824. This database contains a table of the secret keys which are the decoding keys corresponding to the disks' own IDs or the first cipher keys 816 of the IDs, that is the first decoding keys 825 and the IDs. The server can therefore search for the first decoding key 825 based on the received ID. Thus cryptocommunication is completed from the first computer to the second computer 821a. In this case, if the first cipher key and first decoding key are common keys of a common key cipher, not of an public key cipher, they are the same key.

If the user wants to use part of the enciphered contents stored on the disk 801, which may be 1,000 in number, for example, the content number 826 of which is 'n', the user sends to the second computer 821a the cipher which is the content number 826, that is, 'n' enciphered with the public key which is the first cipher key 816 by the first cipher encoder 827 composed of public key cipher functions. The second computer 821a searches for the first decoding key 825 for decoding this cipher as stated above. It is therefore possible securely to convert this cipher into plaintext. Thus, the cipher protects the privacy of the user's order data.

In this case, a signature may be made by means of the secret key of the public key cipher as the first cipher key 816. This method is called 'digital signature'. For a detailed explanation of the operation of 'digital signature', see, for example, 'Digital Signature of E-Mail Security by Bruce Schneider 1995'.

Back to the cryptocommunication, the cipher is sent through the communication part 822 and network 823 to the first cipher decoder 827 of the password issue center 821. Thus the first cipher decoder 827 decodes the cipher by means of the first pair cipher key 825 pairing with the first cipher key 816.

In this case, because only the one disk has the public key, it is possible to reject invalid orders from third parties' disks. In other words, because each disk can be certified, it is possible to certify the user who owns the disk. It is thus certified that the content number 'n' represents a particular individual's order. It is therefore possible to exclude invalid orders of third parties.

If the public key 816 is secret, this method can technically be used to send a credit card number, or other accounting data which requires high security. Generally shops called 'malls' however, do not settle users' accounting data electronically, because there is no guarantee of security. Only the accounting centers 828 of credit card companies, banks and the like can deal with users' financial data. Presently, security standards such as secure electronic transaction (SET) are being unified, so it is probable that Rivest, Shamir and Adleman (RSA) 1024 bit public key ciphers will be used and the encipherment of financial data will be possible.

Next, the accounting data cryptocommunication procedure of the present invention will be shown. First, by using the second cipher key 817 of the public key cipher reproduced by the BCA reproduction part 820, the second cipher encoder 831 enciphers the account-

ing data 830 such as an individual's credit card number with a public key system cipher such as RSA. The enciphered data is sent from the communication part 822 through the second computer 821 to the cipher decoder 832 of the third computer 828. In this case, if there is a need for digital signature, the secret key 829 is used as the second cipher key 817.

Similar to the procedure for the cipher key of the second computer 821a of the password issue center 821, it is possible to search the cipher key database 824a for the second decoding key 829 corresponding to the ID or the second cipher key 817. By using this decoding key 829, the second cipher decoder 832 can decode the enciphered accounting data.

If a digital signature is made by the second cipher encoder 831 with the secret key 829, the user's signature can be confirmed in the second cipher decoder 832. The accounting center 828 can thus get the user's credit card number, bank card number, bank password, or other accounting data safely even via the Internet. In open networks such as the Internet, security comes into question. By means of this system, however, it is possible to make cryptocommunication or certification without fault, because the cipher key (public key) for cryptocommunication or the secret key for digital signature has been recorded in the BCA. It is therefore possible to prevent third parties' unauthorized accounting and orders. In addition, because it is possible to use various public keys for different disks, that is, different users, the confidentiality of communication is improved, and the possibility of users' accounting data leaking to third parties is reduced.

Referring back to Fig. 6, the procedure for issuing a password and the procedure for unlatching with a password will be explained. The password issue center 821 includes a password generation part 834 with an operation expression of public key ciphers etc. Part 834 generates a password on the basis of three data fields, namely, the ID, the content number which the user wants to unlatch, and the time data representing the period of use allowed. The generated password is sent to the first computer 909. In the simplest structure example, the second computer enciphers with the public key for the public key cipher the data which is a mix of the decoding key disk ID for releasing the cipher of the '1- n'th content and the timing data, prepares at the password generation part 834 the '1- n'th password 834a which is a mix of secret keys for unlatching the enciphered data, and sends this password 834a to the first computer 909. The first computer 909 receives the '1- n'th password, and decodes with the secret key the mixed keys of the disk ID, the timing data and the '1- n'th content. Here, the password operation part 836 checks the ID 835a of the BCA reproduced from the disk, the present second timing data 835b, the allowed ID 833a and the first timing data 833, and operates to determine if they coincide. If they do coincide, they are allowed. The '1- n'th decoding key 836a is output to the cipher decoder 837. The cipher 837a of the '1- n'th content is decoded. The '1- n'th content 838 then is output. The period of output is limited to the time during which the first timing data 833 and second timing data 835b coincide. The password operation part 836 of the first computer 909 computes three data fields, which are the ID, the password 835 and the timing data from the clock 836b representing the present time. If the ID and timing data are correct, the correct decoding key is output as the result of the computation. Therefore, the cipher decoder 837 decodes or descrambles the '1- n'th cipher, outputting the plaintext data of the '1- n'th content 838, or a descrambled picture signal or audio signal.

In this case, if the second timing data 835b of the clock 836b does not coincide with the first timing data 838 of the password, the cipher is not correctly decoded and therefore not reproduced. If timing data is used, it can be applied to time-limit type rental systems, so that a movie can be reproduced for only three days during a rental period.

While Fig. 6 shows the procedure in a block diagram, the flowcharts of the procedure will be explained later with reference to Figs. 16 - 23.

Next, the system for the cipher key will be described. By putting, as shown in Fig. 7a, both the first cipher key 816 and second cipher key 817 in the BCA, it is possible to provide two securities, for a commodity deal with a shopping mall and an account settlement with an 'accounting center'.

In this case, with respect to the security with an accounting center, it is planned to unify standards such as SET, so that an RSA 1024, that is 128 byte cipher key, will be stored in the second cipher key area 817a. Then, because the BCA has only 188 bytes, only 60 bytes remain for the cipher key for dealing with a shopping mall. An elliptic function system public key cipher is a cipher function which is 20 bytes in magnitude and which has a security level equal to that of 128 bytes of RSA 1024.

An elliptic function is used in the first cipher key area 816a of the present invention. An elliptic function can obtain 20 byte security, which is equivalent to RSA 1024. Therefore, by using an elliptic function, it is possible to store both the first cipher key 816 and second cipher key 817 in the 188 byte BCA area.

By applying a BCA to an optical ROM disk, as stated before, it is possible to record a disk's own ID number, the first and second cipher keys, and a connection address. In this case, if the Internet is used, a mall is accessed automatically, and merely by distributing disks with cipher keys recorded in the BCAs, security is possible for distribution of commodities by releasing the ciphers of contents, certification and keeping secret purchase of goods, certification and keeping secret when accounts are settled, and the like. Therefore, the method of cryptocommunication of the present invention can, without lowering security, omit and rationalize the conventional operations of using IC cards, floppy disks and/or letters to distribute IDs and/or cipher keys to users. This is a great advantage. Furthermore, a

URL, which is an Internet connection address, is not fixed, but changeable. The URL is recorded in the original disk, and may be accessed. It is, however, not efficient from the points of view of time and cost to vary the original disk when a URL change is made. By having recorded the changed URL in the BCA, and connecting the BCA connection address 931 instead of the connection address of the original disk only if the connection address 931 is reproduced from the BCA, it is possible to access the changed address 931 without preparing a new original disk.

Fig. 6 shows a case where the first key of the public key and the first key of the public key have been recorded in the BCA.

Fig. 8 shows two diagrams, in one of which the first cipher key 816 of the public key and the third decoding key 817a of the secret key have been recorded in the BCA. In the other diagram, a cipher key is produced for cryptocommunication. Because the procedure is similar to that of Fig. 6, only different points will be described. First, in a press factory, the first cipher key 816 and third decoding key 817a are recorded in the BCA. The third decoding key 817a is used to receive the cipher enciphered with the public key from an accounting center. In this case, the reception security is improved.

First, with reference to Fig. 8, a more specific example of cryptocommunication where a cipher key is generated will be described. Because the first cipher key 816 is a public key, it is necessary to record the third decoding key 817a for reception in the BCA. But the BCA has a small capacity. In addition, the public key needs processing time. Therefore, in Fig. 8, the cipher key generation part 838a of the first computer 836 generates a pair of a cipher key and a decoding key for the public key or a common key by means of a random number generator or the like. An example of the common key will be described. A common key K 838 is enciphered with the first cipher key 816 and first cipher encoder 842, and sent to the second computer 821a. The second computer uses the main decoding key 844 to convert this cipher into plaintext by means of the main cipher decoder 843, obtaining a common key K 838a. Because both have the common key K, it is possible to make cryptocommunication from a shop to a user, that is, from the second computer 821a to the first computer 836 by delivering the common key K to the second cipher encoder 842a and second cipher decoder 847a. Naturally, it is also possible to make cryptocommunication from the user to the shop, that is, from the first computer 836 to the second computer 821a by delivering the common key K to the second cipher encoder 827a and second cipher decoder 845a. The effects of the method of recording in the BCA the first cipher key which is a public key and generating a cipher key will be stated. First, it is necessary only to record the first cipher key, so that the recording of the decoding key can be omitted. Therefore, the small capacity of the BCA is not reduced. Second, because the decoding key is recorded in the BCA, the security is improved. The common key may be changed each time.

Because of the short operation time, the processing time is short. In this case, if the cipher key generation part 838a has generated a pair of a cipher key and a decoding key of a public key cipher, not a common key, it is possible to make the security higher than that with the common key, though the processing time is longer, by cryptically sending the cipher key to the second computer 821a, using this key as the cipher key of the second cipher encoder 842a, and using the decoding key as the decoding key of the second cipher decoder 847. If the performance of the processing CPU is high, it is preferable that the public key be used. If a new public key is generated, only the public key for the first cipher key is recorded in the BCA, so that no problems of security arise. No capacity of the BCA is consumed either. In addition, because it is not necessary to change the cipher key, maintenance is easy.

This time, if the common key K 838 is defined at the second computer 821a of the password issue center 821, the common key is enciphered with the third cipher key 839 by the third cipher encoder 840, and sent to the personal computer 836. By using the third decoding key 837 which is the secret key reproduced from the BCA, the third cipher decoder 841 of the personal computer 836 makes a translation into plaintext to obtain a common key K 838b. In this case, because only this user has the third decoding key 817a which is the secret key, it is possible to prevent the contents of communication from the center to the user from leaking to third parties. The format of this case is shown in Fig. 7b. If an elliptic function is used, the third decoding key 839b may be 20 bytes, and can therefore be stored in the BCA.

Fig. 9 shows a system for reducing the costs of preparing an original disk by using a BCA in an encipherment disk.

If there is a number 'n' of, for example, 1,000 plaintext contents 850, the cipher encoder 852 enciphers them with the first to the 'm'th cipher keys 851, respectively. The ciphered first to the 'm'th contents 853, the decoding program 854a for the first to 'm'th contents, and the second cipher decoder 861a, which is the program for decoding the second cipher, are recorded as pits in an original disk and then molded into a substrate, and a reflecting film is formed. Thereafter, two substrates are laminated together to complete an optical disk 801. The second cipher encoder 860 enciphers the decoding data 854 such as the password for unlatching the '1- n'th, for example, the first content, and the decoding key. Recorded in advance in the BCA of the first disk are the disk's own identification data, that is, the ID 855 and the second cipher which is the enciphered decoding data. Then, in the reproducer, the second cipher is reproduced from the BCA reproduction part 820. The second cipher decoder 861 is reproduced from the data reproduction part 862, which reproduces the ordinary recorded data other than the BCA. Therefore, the second cipher decoder 861 is used to decode the second cipher, reproducing the ID 855a and '1- n'th password

854a. The cipher decoder 855b uses the decoding program 854a for the '1- n'th content reproduced from the data reproduction part 862, and uses the ID 855a and password 854a to decode the first cipher, obtaining the plaintext 855c of the '1- n'th content and the identification data 855a. For a personal computer, the content and ID are recorded on the hard disk 863. This ID 855a checks to determine if there is no same ID on a network when the program has started, and the ID 855a actuates the network protection. It is therefore possible to prevent the software from being illegally installed. This is yet another advantage of the present invention. For example, if 1,000 enciphered contents are stored and decoding data such as a password corresponding to a particular software application are recorded on an original disk, this is equivalent in substance to the preparation of an optical ROM disk for a particular content. It is possible to obtain with one original disk the same effect as in the case where original disks for 1,000 kinds of software are cut. It is therefore possible to reduce the costs and time or labor for preparing an original disk.

Described with reference to Fig. 10 is the procedure for enciphering contents with a BCA when recording them on a RAM disk. First, the BCA reproduction part 820 reproduces the BCA data from the RAM disk 856, outputs an ID 857, and sends it through the interfaces 858a and 858b and the network to the encipherment part 859. The cipher encoder 861 of the encipherment part 859 enciphers contents 860 or scrambles picture and sound signals by means of a key including the ID 857. The enciphered contents are sent to the recorder/reproducer, where the recording circuit 862 records them on the RAM disk 856.

Next, when this signal is reproduced, the data reproduction part 865 demodulates the main data to reproduce the enciphered signal, and the cipher decoder 863 decodes the reproduced signal. The BCA reproduction part 820 reproduces data containing the ID 857 from the BCA area of the RAM disk 856. The reproduced data is sent as part of the key to the cipher decoder 863. If normally copied, the cipher key recorded in the RAM disk is a normal disk ID. The RAM disk ID, also, is a normal disk ID. Therefore, the cipher is decoded or descrambled to output the plaintext 864 of the '1- n'th content. For a graphic data, for example, the MPEG signal is extended to obtain a picture signal.

In this case, the disk ID is the key for encipherment. Because each disk is unique, it can be copied on only one RAM disk.

If a disk ID is copied from a normal RAM disk to another RAM disk, ID1 which is the original normal disk ID differs from ID2 which is the disk ID of the other, unauthorized, RAM disk. If the BCA of the unauthorized RAM disk is reproduced, ID2 is reproduced. The contents are ciphered with ID1, however, so that, even if unlatching is attempted with ID2 at the cipher decoder 863, the cipher is not decoded because the key differs. Thus, the signal of the illegally copied RAM disk is not output, so that the copyright is protected. The present invention uses a disk ID system. Therefore, by reproducing with any drive the normal RAM disk copied normally only once, it is possible to unlatch the cipher. The encipherment part 859 may, in place of the center, be an IC card with a cipher encoder.

With reference to the block diagram of Fig. 11 and the flowchart of Fig. 12, the method of preventing copying will be described. At Step 877a, the installation program is actuated. At Step 877b, the BCA reproduction part 820 outputs the ID of the auxiliary data from the laminated optical disk 801. At Step 877d, the data reproduction part 865 reproduces the contents and network check software 870 from the main data. The contents and the ID 857 are recorded on the HDD 872. At Step 877c, the ID 857 is encoded with a particular secret cipher so as not to be altered illegally, and is recorded as a soft ID in the HDD 857. Thus, the soft ID 873 is recorded together with the contents on the HDD 872 of a personal computer 876. Here described is the case where the program is started at Step 877f of Fig. 12. When the program is started, the procedure goes to Step 877g, where the soft ID 873 of the HDD 872 is reproduced, and the soft ID 873a in the HDD 872a of another personal computer 876a on a network 876 is checked through the interface 875. At Step 877h, a check is made to judge if the soft ID 873a of the other personal computer and the soft ID 873 are the same number. If so, the procedure goes to Step 877j, where the start of the program of the personal computer 876 is stopped or a warning message is displayed on the screen.

If the soft ID 873a of the other personal computer and the soft ID 873 are different, the contents are not installed in the plurality of the computers on the network. It is therefore decided that there are no illegal copies. Then the procedure goes to Step 877k, where the start of the program is permitted. In this case, the soft ID 873 may be sent to other personal computers through the network. This personal computer can detect illegal installation by checking duplication of the soft IDs of the personal computers. If there is illegal installation, a warning message is sent to the appropriate personal computer/s.

Thus, by recording the ID in the BCA, and recording the network check program in the pit recording area, it is possible to prevent multiple installation of the software of the same ID on the same network. In this way, simple protection from illegal copies is realized.

By, as shown in Fig. 13a, applying a write (writing) layer 850 of white material, on which characters or the like can be written, it is possible to not only print characters and write a password or the like with a pen, but also prevent the substrates of the optical disk from being damaged because the write layer 850 thickens. The disk ID 815, which is part of the BCA data 849 recorded by trimming in the BCA area 801a above the write layer 850, is translated into plaintext. The plaintext is converted into alphanumeric characters 851. By printing the characters 851 and general bar code 852, it is pos-

sible for the store and/or user to confirm and/or check the ID with a POS bar code reader and/or visually, without reading the BCA with a reproducer. The visible ID is not necessary if the user informs the center of the ID through a personal computer. If, however, the user communicates the ID aurally by telephone to the center, it is possible to inform the center of the ID without inserting the disk in a personal computer, by printing the ID identical with the BCA ID in visible form on the disk, because the user can visually read the ID. With reference to the flowchart of Fig. 13c, the steps for making an optical disk will be explained. At Step 853d, disks are molded from an original disk, and substrates in which pits have been recorded are made. At Step 853e, aluminum reflection films are made. At Step 853f, two disk substrates are laminated with an adhesive so that a DVD disk or the like is completed. At Step 853g, a label is printed by screen printing on one side of each disk. At this step, the original disk's own identification data is recorded in the form of a bar code. At Step 853h, an ID and/or other identification information is printed in the format of a bar code for POS on each disk by an ink jet bar code printer or a thermal-transcription bar code printer or the like. At Step 853i, the bar code is read by a bar code reader. At Step 853j, a BCA data corresponding to the identification data is recorded in the second recording area of the disk. According to this method of manufacturing, the BCA data is recorded after all the steps including the POS bar code and excluding the BCA are finished and then the disk identification data is confirmed. The BCA can be read only by reproducing the disk, but the POS bar code, which is low in density, can be read by a commercial bar code reader. The disk ID can be discriminated at every step in the factory. By recording the disk ID in the form of a POS bar code before the BCA trimming, it is possible to almost completely prevent the BCA and the POS bar code from being illegally recorded.

The method of using a BCA will be stated by which secondary recording and tertiary recording, too, can be made by the BCA method. As shown at Process 2 in Fig. 15, a software maker can also secondarily record a pirated edition prevention mark and a check cipher. At Process 2, disks 944b may be made in which different ID numbers and/or cipher keys for secret communication with users have been recorded. It is possible to replay the disks 944c and 944d without entering the passwords.

For another application, at Process 3, an enciphered or scrambled MPEG picture signal and/or other data is recorded on a disk 944e. The operation of the MPEG scramble will not be explained in detail. At Process 4, the software company makes a disk 844f in which a sub-public key for decoding the ID number and the scramble release data have been BCA-recorded secondarily. It is not possible to replay this disk solely. At Process 5, the selling store, after receiving the money for the disk, makes a password with the sub-secret key paired with the sub-public key, and records it tertiarily on the disk. Alternatively, a receipt on which the password has been printed is given to the user. Thereafter, the password has been recorded in the disk 844g, so that the user can replay it. This method prevents a disk not paid for from being replayed normally, even if the disk is shoplifted, because the scramble of the image is not released. As a result, shoplifting renders a useless product and thus decreases.

If a password is BCA-recorded permanently in a rental video store or another store, a shoplifted disk can be used. In this case, as shown at Process 6, the BCA is read by a POS bar code reader in the store. A password for releasing the scramble is issued at Step 951g, printed on the receipt at Step 951i, and handed to the customer at Step 951j. The customer enters, at Step 951k, the password on the receipt in a player with numeric keys at his/her house. At Step 951p, the disk is replayed for a predetermined number of days. If a user rents a disk, given a password for only part of the software in the disk, and when he/she wants to view other part of the software, he/she can replay it by being informed of the password for this part by telephone at Step 951u, and entering the password at Step 951k. A rental video store has been shown as an example. When a piece of enciphered software for a personal computer is sold at a personal computer software store, the password may be printed by a POS terminal and handed to the buyer.

The operations of Processes 5 and 6 in Fig. 15 at a selling or rental store will be explained in more detail with reference to Fig. 14. A selling store receives an enciphered and/or scrambled disk 944f from the software maker. After the store confirms its receipt of money from a user, it sends from its bar code recorder 945 the ID number of the disk 944f and the data on the sub-public key via its POS terminal 946 to the password issue center 952. For a small-scale system, the password issue center, that is, the system including the sub-secret key of the sub-public key may exist in the POS terminal. The password issue center inputs the disk ID number and the time data at Step 951q, computes them at Step 951s, enciphers them with the sub-secret key at Step 951t, issues a password at Step 951g, and sends it through the network 948 and POS terminal 846 to the BCA bar code recorder 945. Then the recorded disk 944g is handed to the customer. The disk 944g can be replayed as it is.

For rental stores and personal computer software stores, ROM disks 944f the ciphers and/or scrambles of which have not been released are displayed in stores. If a customer designates a particular ROM disk 944f, the bar code of the reflection layer by the non-reflection part 915 of the disk 944f is read, so that the disk ID number is read, by a person holding a circular bar code reader 950 with an integrated rotary optical head 953 for spirally scanning, and pressing it on the center of disk 900 in a transparent case. By printing the commodity bar code of the disk ID as shown at 852 in Fig. 13, it is possible to read the code with an ordinary POS terminal bar

code reader. Alternatively, the pressed circular bar code recorded in advance on the original disk may be read. These data including the disk ID are processed by the POS terminal 946. The charge is settled by credit card. The password issue center issues, at Step 951g, a password associated with the ID number as stated above. For rental use, a password is made by enciphering the disk ID number with date data added as used at Step 951r in order to limit the number of days for which the disk can be replayed. For this password, the disk can operate on only particular days. It is therefore possible to set a rental period, which may be three days, for instance, in the password.

The thus issued password for descrambling is printed at Step 951i together with the date of rent, the date of return and the rental title charge on the receipt 949, and handed with the disk to the customer. The customer takes the disk 944j and receipt 949 home. At step 951k, the customer enters the password with the ten-key input part 954 of the first computer 909 in Fig. 6, so that the password 835 is computed with the ID number 835a and input into the cipher decoder 837. Then, the password is converted into plaintext by means of the decoding key. Only if the password is correct, will the cipher decoder 837 descramble the program data and supply image output.

In this case, if the password includes time data, the data is checked with the date data of the clock part 836b. The password is descrambled for the coincident dates. The inputted password is stored together with the associated ID number in the nonvolatile memory 755a of the memory 755. Once the user enters the password, it is descrambled without being entered again. It is thus possible to lock and unlock the disk electronically in distribution.

With reference to Fig. 16, the method of decoding the software of a disk which has been recorded as cipher data will be explained in detail.

Step (Process) 865 represents the overall flow of distribution of cipher data and individual IDs to users. First, at Step 865a, a number 'm' of data enciphered with the secret first cipher key and a program for decoding the enciphered data are recorded in the ROM area of an original disk. At Step 865b, substrates are molded from the original disk, and then the substrates with reflection films added thereto are laminated in pairs to make completed ROM disks. At Step 865c, the decoding data (the disk identification data different for the pressed disks, respectively, and/or the decoding key for the cipher data) necessary to decode the enciphered data is recorded in the auxiliary recording area (called BCA), which cannot be rewritten, of each completed disk by a method of modulation different from that for the ROM area. At Step 865d, a user replays the distributed disk, selects a desired enciphered data 'n', and starts the decoding process. At Step 865e, the user's first computer reproduces the enciphered data and the decoding program from the ROM area, and reads the decoding data from the auxiliary recording area (BCA). If, at Step 865f, the second decoding data is not obtained on-line, then, at Step 871a of Fig. 17, the ID and/or other auxiliary decoding data are displayed on the screen. At Step 871b, the user obtains the second decoding data such as the password associated with the ID, and enters it into the first computer. Carried out at Step 871c is a particular operation of an open-key cipher function with the disk identification data, the second decoding data, and the enciphered data 'n' If, at Step 871d, the result is correct, then, at Step 871f, the '1- n'th data is translated into plaintext, so that the user can make the software of the data 'n' operate.

Next, with reference to the flowchart of Fig. 18, the method of cryptocommunication essential to the Internet and/or the like using a BCA will be described. Step (Process) 868 is the routine of the method of distributing the communication program and cipher key for communication to users. First, at Step 868a, at least the communication program and/or connection data are recorded in the ROM area of an original disk. At Step 868b, substrates are molded from the original disk, and the substrates are laminated in pairs to make completed ROM disks. At Step 868c, the disk identification data different for the pressed disks, respectively, and the cipher key for cryptocommunication are recorded in the non-rewritable auxiliary recording area (BCA) of each completed disk. According to circumstances, the connection address of the second computer and/or the decoding key for cryptocommunication is recorded by a method of modulation different from that for the ROM area. At Step 868d, the user's first computer reproduces the communication program and the decoding program from the ROM area, and reads the disk identification data and the cipher key for communication from the auxiliary recording area. The process continues at Fig. 19. At Step 867a, it is judged if there is a connection address in the BCA area. If yes, the second computer is accessed, at Step 867b, on the basis of the connection address such as the BCA area URL. If there is no connection address, the computer of the connection address in the ROM area is accessed at Step 867c. At Step 867d, the transmit data is input. At Step 867e, it is judged if there is a cipher key for cryptocommunication in the BCA area. If so, the transmit data is enciphered, at step 867g, with the cipher key for cryptocommunication in the BCA area to make a third cipher. If not, the data is enciphered, at step 867f, with the cipher key for cryptocommunication in the ROM area or HDD to make a third cipher.

In Fig. 20, Step (Process) 869 represents the routine of generating a decoding key for the cipher received from the second computer 910. First, at Step 869a, the first computer judges if a decoding key for communication is necessary. If necessary, the process goes to Step 869b, where a check is made to judge if there is a decoding key for communication in the BCA. If there is no decoding key, the process goes to Step 869c, where a pair of second cipher key for communication and second decoding key for communication is generated newly

with the program for generating the cipher key/decoding key reproduced from the ROM area, by the user keying or with data from a random number generator and the second encoder reproduced from the ROM area. At Step 869d, a fourth cipher is made which is the second cipher key for communication and/or the user data enciphered with the cipher key for communication recorded in the BCA and the encipherment software reproduced from the ROM area. At Step 869e, the fourth cipher and the disk identification data and/or the user address are sent to the second computer of the connection address reproduced from the disk. The process of the second computer includes Step 869f, where the fourth cipher, the disk identification data and the user address are received. At Step 869g, the decoding key for communication paired with the disk identification data is selected from the decoding key data base, and the fourth cipher is decoded with the selected key to obtain the plaintext of the second cipher key for communication. At Step 869h, the fifth cipher which is the server data including part of the user data and enciphered with the second cipher key for communication is sent through the Internet 908 to the first computer. At Step 869i, the fifth cipher (and disk identification data) is (are) received, and decoded with the second decoding key for communication and the decoding function recorded in the ROM area to obtain the plaintext of the server data. In this way, the method of Step 869 in Fig. 20 realizes two-way cryptocommunication between the first and second computers.

In Fig. 21, Step (Process) 870 represents the routine of receiving accounting data. If, at Step 870a, the accounting data is input, the third cipher key of the public key cipher for accounting communication is requested from the second computer. At Step 870b, the second computer requests the third cipher key from the third computer. The third computer 911 sends the ID and third cipher key to the second computer, though the exchange step is omitted. At Step 870c, the second computer receives the ID and third cipher key. At Step 870e, the seventh cipher which is the third cipher key enciphered with the second cipher key for communication and/or the like is sent to the first computer. The first computer receives the seventh cipher at Step 870f. At Step 870g, the received seventh cipher is decoded with the second decoding key for communication so as to obtain the third cipher key (public key of public key function). At Step 870h, the third cipher key is recorded on the HDD according to circumstances. This is used for the next transmission. At Step 870i, it is judged if a credit card number, a password for settlement and/or other secret accounting data are input. At Step 870j, the eighth cipher which is the accounting data enciphered with the third cipher key is sent via the second computer to the third computer. At Step 870k, the second computer receives the eighth cipher and transfers it again to the third computer. Only the third computer 912, which is, for example, at a banking institution, has the decoding key for the third cipher, so that the second computer, which is an electronic store, cannot decode it. At Step 870m, the third computer determines from the cipher key data base the third decoding key associated with the third cipher key by using identification data on the disk and/or the like, and decodes the eighth cipher with the third decoding key, which is the secret key of the public key cipher, so as to obtain the plaintext of the accounting data. At Step 870n, a check is made to judge from the user's credit data, deposit remains and/or other banking data whether the money can be received. At Step 870p, the third computer informs the second computer of the result of the search. The second computer, which is an electronic store, judges at Step 870q if the money can be received. If not, the process goes to Step 870r, where the article and/or the key for decoding the cipher software is not sent. If the money can be received, for a key provision system as shown in Fig. 16, the process goes to Step 870s, where the cipher software decoding key, that is, the article is sent via Internet 908 to the user's second computer. At Step 870t, the first computer receives the cipher software decoding key. At Step 870u, the cipher of the '1-n'th enciphered software is released. At Step 870w, the plaintext of the software is obtained. In this way, a content key provision system is realized.

The method of Step 870 in Fig. 21 requests the third computer, that is, a banking institution to issue according to the need a public key for the third cipher key, which needs high security for accounting data. It is not necessary to record the public key in the BCA in advance. It is therefore possible to use for the third cipher key a stronger RSA system cipher key of 256 bytes of RSA2048 without consuming the BCA capacity. Further, because there is no need for recording in the BCAs of all disks in advance, the total of the issued third cipher keys decreases, and the computer CPU time taken to compute the third cipher keys decreases. In addition, because the third ciphers do not exist in the BCAs, they are not opened, so that the security is improved. In this case, the role of the BCA is, as shown in Figs. 19 and 20, to record the identification data of a secret communication disk by means of the cipher key of the RSA1024 grade. Only one BCA disk realizes cryptocommunication with the second computer, so that the effect is high.

With reference to Fig. 22, Step (Process) 872 of cryptocommunication in a case where the cipher key and the decoding key both for communication have been recorded in the BCA will be described. At Step 872g, the first computer 909 sends to the second computer 910 the ninth cipher which is the user data enciphered with the cipher key for communication reproduced from the BCA, the basic identification data recorded in the ROM area when the original disk was made, and the disk identification data recorded in the BCA area. At Step 872b, the second computer receives the ninth cipher, the disk identification data and the basic identification data. At Step 872c, the decoding key for communication paired with the disk identification

data from the decoding key data base is retrieved, and the ninth cipher is decoded to obtain the plaintext of the user data. At Step 872e, the second cipher key associated with the disk identification data is selected from the cipher key data base. In addition, the second computer sends to the first computer the tenth cipher which is the server data enciphered with this second cipher and the third cipher key received from the third computer by the procedure described in Fig. 21 and enciphered with the second cipher. The first computer receives the tenth cipher at Step 872f. At Step 872g, the received seventh cipher is decoded with the second decoding key for communication recorded in the BCA, to obtain the plaintext of the server data and the third cipher key (public key of the public key function). At Step 872h, according to the need, the third cipher key is recorded on the HDD. At Step 872i, it is judged if the accounting data is input. If so, the process goes to Step 872j, where the eleventh cipher which is the accounting data enciphered with the third cipher key is sent via the second computer to the third computer. At Step 872m, the second computer sends the eleventh cipher again to the third computer. At Step 872m, the third computer determines from the third cipher key data base, the third cipher key paired with the identification data on the disk and/or the like, and decodes the eleventh cipher to obtain the plaintext of the accounting data. At Step 872n, the possibility that the money can be received from the user is checked. At Step 872p, the result of the search is sent to the second computer. At Step 872q, the second computer checks to judge if the money can be received from the user. If so, for a key provision system as shown in Fig. 16, the process goes to Step 872s, where the cipher software decoding key, that is, an article is sent via the Internet to the user's second computer. At Step 872t, the first computer receives the cipher software decoding key. At Step 872u, the cipher of the '1- n'th enciphered software is released. At Step 872w, the plaintext of the software is obtained. In this way, a content key provision system is realized.

The merit of the effect of the method of Step 872 in Fig. 22 is that, because both the cipher key and the decoding key are recorded in the BCA area, it is not necessary to transmit the decoding key and/or the cipher key necessary for reception from the second computer. The maximum BCA capacity is 188 bytes. A public key and/or another cipher function needs only 128 bytes, and can therefore be recorded. Further, it is possible to bidirectionally encipher the grade in RSA512. Because seven or eight elliptic functions can, as shown in Fig. 7, be stored, elliptic functions are more effective.

With reference to Fig. 23, the operation and effect in a case where the first and third cipher keys have been recorded in the BCA in advance will be explained. Because Steps 872a through 872w in Fig. 22 are nearly identical with Steps 873a through 873w in Fig. 23, only the different steps will be explained.

The third cipher key for protecting the security for accounting data and/or other banking data has been recorded in the BCA. Therefore, at Step 873e, the second and third computers do not need to generate and send the third cipher key. At Steps 873e, 873f and 873g, the twelfth cipher is sent and received. At Step 873j, the third cipher key is read from the BCA area, and the user's accounting data is sent via the second computer to the third computer. The method of Fig. 23 does not need the third cipher key generated, sent and received at all, so that the procedure is simple.

In the case of electronic settlement systems, in general, there are a plurality of accounting centers representative of credit companies. Therefore, naturally, there is a need for a plurality of third cipher keys, which are public keys. As explained with reference to Fig. 7b, there is a need for an RSA1024 grade or more, that is, 128 bytes or more if an RSA cipher function is used. The third cipher key 817b can therefore enter only one place of 188 bytes of the BCA. However, elliptic-function cipher keys (elliptic ciphers) which have appeared in recent years give, with small capacity, security equivalent to that of RSA. In recent years, RSA function RSA1024 has been the lowest standard of banking data security. While an RSA function needs 128 bytes, it is said that an elliptic cipher needs only about 20 through 22 bytes for equivalent security. Therefore, as shown in Fig. 7c, it is possible to store in the BCA seven, eight or fewer third ciphers which deal with banking data. The use of elliptic functions realizes a BCA-application electronic settlement system which can deal with a plurality of essential banking centers. Explanation has been made, concentrated on the third cipher, but even if an elliptic cipher is used for the public key for the first cipher key, its effect is similar because high security is kept in relation to a plurality of electronic stores.

With reference to Fig. 24, the RAM disk recorder/reproducer with a BCA explained with reference to Fig. 10 will be described in more detail. As an embodiment, the procedure for recording in a RAM disk in a so-called pay-per-view system will be described. First, with its program transmitter 883, a CATV company or another software company enciphers movie software or other contents 880 by using the first cipher key 882 in the first encoder to generate a first cipher 900, and sends this cipher to a decoder 886 such as each user's CATV decoder. If the decoder 886 sends a request for a particular program through a network to a key issue center 884, the center sends the first decoding data 885a to the first decoding part 887 of the first decoder 886. The first decoding data 885a is a particular piece of software such as the scramble release key for the particular decoder system ID number and particular timing data 903, and includes a recording permission card 901 for a RAM disk. The first decoding part 887 decodes the first cipher 900 with the system ID 888 and first decoding data 885a. In the case of a picture signal, the signal descrambled once and scrambled further with another cipher to protect the signal from being copied is output from the third cipher output part 889. The picture can be

viewed and listened to on a general TV 899, though the original signal is guarded from being copied. If the recording permission code 901a is NO, it is not possible to record in a RAM disk 894. If OK, however, it is possible to record in only one RAM disk 894. This method will be explained.

In the decoder 886, an IC card 902 is inserted, and the BCA reProduction part 895 reads the BCA of the RAM disk 894 in a RAM recorder. Then the disk ID 905 is sent to the IC card 902. The IC card 902 checks the recording permission code 901a and the present time data 904 obtained from the disk IC 905 and the decoder 886, and makes a two-way hand-shake type copy check 907 with the third cipher output part 889. If the recording permission code and copy checks are OK, the second auxiliary encoder 891 in the IC card 902 issues a second cipher key 906. The second encoder 890 enciphers the third cipher again to generate a second cipher, which is the contents 880 enciphered with the disk ID of a particular disk. The second cipher is sent to the RAM recorder 892, where it is 8-15 or 8-16 modulated by the first modulation part in the recording means 893. The second cipher 912 is recorded in the first recording area 894a of the RAM disk 894 by means of a laser. In this way, the data of the RAM disk 894 is enciphered with the particular disk ID number.

When the reproduction signals in this disk are 8-16 demodulated by the first modulation 896a using a normal reproduction means 896, the second cipher of the contents is output. The second decoder 897 has second decoding keys 898a, 898b and 898c, which correspond to the cipher keys of the IC cards different for CATV stations or other program supply companies, respectively. In this case, the decoding key identification data of the decoder 868 or IC card 886 has been recorded in the first recording area 894a. The reproducer reads the decoding key identification data 913 from the first recording area 894a. The decoding key selection means 914 automatically selects out of the decoding keys 898a through 898z the second decoding key 898a corresponding to each cipher key. With the disk ID 905a as a key, the second decoder 897 decodes the second cipher. An IC card having a particular decoding key might be used. In the case of an image, it is possible to obtain a normal image descrambled at a TV 899a.

In the system of Fig. 24, a disk ID 905 is sent to the IC card inserted into the decoder in each user's home to encipher picture image data and/or the like. It is therefore not necessary for the software company 883 to individually change the cipher of the contents for distribution to users. Consequently, when broadcasting scrambled pay-per-view images to a great number of viewers as is the case with satellite broadcasting and CATV, it is possible to permit recording in only one RAM disk per user.

If, at the same time when recording is made in a disk in the system of Fig. 24, an attempt is made to illegally copy, that is, record in a second disk, that is, a RAM disk of another disk ID, it is not possible to alter the disk ID because two-layer disks are used for BCAs. Therefore, unauthorized copying in the second disk at the same time is prevented. It can be considered that during another time period, a simulated or dummy recording permission code 901a and/or a third cipher is sent to the decoder and/or IC card and data is recorded in a RAM disk of another disk ID. Even against such unauthorized practice, the decoder time data control part 902 in the IC card compares the time of the timing data 903 of the key issue center 884 and/or the time of the time data of the contents and the present time of the time data part 904a in the decoder to judge if they coincide. If so (OK), the IC card 902 permits the encipherment of the second cipher computing unit 990.

In this case, a hand-shake type time check method might be used which makes the second encoder 890 and first decoder 887 exchange check data bidirectionally.

In the case of the hand-shake type, the second cipher computing unit 890 including the IC card, the first decoding part 887, and the third cipher part 889 confirm the cipher data bidirectionally. This prevents the unauthorized copying during the other time periods outside the time when the contents are sent.

In this way, in each user's decoder 886, the software company's contents are recorded in only one RAM disk 894 for each particular disk ID. This disk can be reproduced by any RAM disk reproducer. Even in the case of recording in a RAM disk by the method of Fig. 24, the software company's copyright is protected. Althoughthe encipherment and decoding have been explained with reference to the cipher encoders and cipher decoders, respectively, in the detailed description of the drawings, the cipher algorithm and the decoding algorithm are practically used with programs in a CPU.

## INDUSTRIAL APPLICABILITY

By thus recording in advance the cipher key and/or the decoding key for an ID and/or a cipher in the BCA area of an optical disk, it is possible to release the cipher of enciphered contents by a simpler procedure. In addition, the secrecy of communication is realized without a conventional procedure for registration. By storing a network check program in contents, it is possible to prevent pieces of software of the same ID on the same network being installed. Thus, there are various effects on the improvement of security.

## REFERENCE NUMERALS

801: disk with a BCA
802: fixed key
803: cipher encoder or scrambler
804: recording means
805: contents
806: ID
807: trimming unit
808a: molding machine

808b: reflecting film making machine
808c: bonding machine
809: completed disk
809a: single-sided disk
809b: single-sided disk
811: press field
813: fixed key
814: BCA area
815: disk ID
816: first cipher key (secret key)
817: second cipher key (secret key)
818: connection address
819: reproducing unit
820: BCA reproducing section
821: password issue center
822: communication section
823: network
824: cipher key DB
825: first decoding key
826: contents number
827: first cipher decoder
828: accounting center
829: second decoding key
830: accounting data
831: second cipher encoder
832: second cipher decoder
833: timing data
834: password producing section
835: password
836: personal computer
837: third decoding key
838: common key
839: third cipher key
840: third cipher encoder
841: third cipher decoder
842: main cipher encoder
843: main cipher decoder
844: main decoding key
845: first cipher decoder
846: cipher encoder
847: cipher decoder
849: BCA data
850: writing layer
851: character
852: general bar code
853: decoder
860: second cipher encoder
861: second cipher decoder
862: data reproducing section
863: ROM area
864: additional recording area
865: decoding flowchart
890: second cipher computing unit
894a: first recording area
908: Internet
909: first computer
910: second computer
911: third computer
912: second cipher
913: decoding key identifying data
914: decoding key selecting means
915: first slice level
916: second slice level
917: PE-RZ modulator
918: transparent substrate
919: first recording area
920: second recording area
921: disk ID
922: BCA flag
923: CPU
924: control data
925: EFM demodulation
926: 8-15 modulation-demodulation
927: 8-16 modulation-demodulation
928: first demodulating section
930: second demodulating section
931: connection address

## Claims

1. An optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a plurality of radially long parts of a reflection film are removed partially, so that auxiliary data are recorded by a second method of modulation, which differs from the first method, the optical disk being characterized by:

   the auxiliary data including a first identification data recorded therein for identifying individual optical disks; and
   the main data including an impermissible part recorded therein which can be used with the first identification data and/or a specified password.

2. The optical disk described in Claim 1, and further characterized in that it is a read only type optical disk.

3. The optical disk described in Claim 1 or 2, and further characterized by a specified password being obtained through a specified operation with the first identification data.

4. The optical disk described in Claim 1 or 2, wherein, in addition to the first identification data for identifying individual optical disks, a cipher key for a cipher and/or a decoding key for a cipher is recorded in the auxiliary data.

5. The optical disk described in Claim 1 or 2, and further characterized by the first method of modulation being a method of 8-16 modulation, and the second method of modulation being a method of phase encoding modulation.

6. A method of permitting the use of a program, the method being characterized in that it comprises the steps of:

reproducing an optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a plurality of radially long parts of a reflection film are removed partially, so that auxiliary data are recorded by a second method of modulation, which differs from the first method, the auxiliary data including a first identification data recorded therein for identifying individual optical disks and a cipher key for a cipher and/or a decoding key for a cipher, the main data including an impermissible part recorded therein which can be used with the first identification data and/or a specified password;
reproducing the first identification data from the auxiliary data; and
enabling the impermissible part to be used and outputting it with the first identification data and/or the specified password.

7. The method of permitting the use of a program described in Claim 6, and further characterized by the specified password being obtained through a specified operation with the first identification data.

8. A method of cryptocommunication characterized in that it comprises the steps of:

reproducing in a first computer an optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a plurality of radially long parts of a reflection film are removed partially, so that auxiliary data are recorded by a second method of modulation, which differs from the first method, the auxiliary data including a first identification data recorded therein for identifying individual optical disks and a first cipher key for a cipher and/or a decoding key for a cipher;
reading the first identification data and the first cipher key from the auxiliary data;
obtaining a first cipher which is a first data enciphered with the first cipher key and cipher algorithm; and
sending the first cipher from a communication means of the first computer through a network to a second computer.

9. The method of cryptocommunication described in Claim 8, and further characterized by the cipher algorithm being read from the main data.

10. A method of cryptocommunication characterized in that it comprises the steps of:

reproducing main data from a first recording area of an optical disk in a first computer;
reproducing auxiliary data from a second recording area, the auxiliary data including a first identification data for identifying individual optical disks and a first cipher key for a cipher and/or a decoding key for a cipher;
enciphering a first data in the first computer with the first cipher key in the auxiliary data by cipher algorithm to make a first cipher;
connecting to the second computer of a particular connection address through a network to send the first cipher and the first identification data in the auxiliary data;
receiving the first identification data and the first cipher in the second computer;
selecting the first decoding key which is the decoding key for the cipher corresponding to the first identification data received from a first decoding key database, where a relationship between the first decoding key and the first identification data is stored; and
decoding the first cipher on the basis of the first decoding key to obtain the first data.

11. The method of cryptocommunication described in Claim 10, and characterized in that it comprises the further steps of:

generating with a first means for generating ciphers in the first computer a second cipher key and a second decoding key paired with each other;
obtaining a third cipher which is the second cipher key enciphered with the first cipher key in the first computer; and
sending the third cipher to the second computer.

12. The method of cryptocommunication described in Claim 11, and characterized in that it comprises the further steps of:

decoding the received third cipher with the first decoding key to obtain the plaintext of the second cipher key in the second computer;
obtaining a fourth cipher which is the second data enciphered with the second cipher key; and
sending the fourth cipher to the first computer.

13. The method of cryptocommunication described in Claim 8, and further characterized in that, at the step of reproducing two or more cipher keys and/or

decoding keys for public key cipher from auxiliary data which include public key cipher, at least one of the cipher keys and the decoding keys is an elliptic function cipher.

14. The method of cryptocommunication described in Claim 8, and characterized in that it comprises the further step of using an optical disk with auxiliary data including a connection address data of the second computer, and reproducing the connection address from the auxiliary data.

15. An optical disk recorder for modulating a main data by a first method of modulation and recording the data by radiating a laser beam through an optical lens on to the recording layer of a first recording area of an optical disk, the recorder being characterized by:

reproducing, before recording, the auxiliary data in a second recording area, where a first identification data and a first cipher key for a cipher and/or a decoding key for a cipher are recorded by a second method of modulation;
making a main cipher which is the main data enciphered with the first identification data and/or the first cipher key and particular cipher algorithm; and
recording the main cipher in the recording layer of the first recording area by the first method of modulation.

16. The optical disk recorder described in Claim 15, and further characterized by:

receiving in a reception part the second cipher which is the first data enciphered with second cipher algorithm and a recording permission data permitting recording the first data in an optical disk;
obtaining a second decoded data through decoding the second cipher with a second decoding means;
making a main cipher through enciphering the second decoded data with first cipher algorithm different from the second cipher algorithm and an auxiliary data in a cipher computing means; and
recording the main cipher in the first recording area of the optical disk only if the recording permission data is present.

17. The optical disk recorder described in Claim 16, and characterized by:

mounting an IC card having a computing unit therein;
inputting into the IC card the first identification data for identifying the disk of the auxiliary data;
computing the first identification data with the computing unit;
inputting the result of the computation into the cipher computing means from the IC card;
obtaining a main cipher which is an enciphered second decoded signal; and
recording the main cipher in the optical disk.

18. An optical disk reproducer characterized by

reading with an optical head and a first means of demodulation an optical disk including a first recording area, where a main cipher is recorded by a first method of modulation, the main cipher being a first data enciphered with a first identification data by a cipher means;
reproducing with the optical head and a second means of demodulation an auxiliary data recorded in a second recording area of the optical disk by a second method of demodulation; and
obtaining the first data by decoding the main cipher by means of the decoding means with the first identification data in the auxiliary data or a first auxiliary identification data which is obtained from the first identification data through a predetermined computation.

19. The optical disk reproducer described in Claim 18, and further characterized by the method of modulation-demodulation of the first means of demodulation being a method of 8-16 modulation-demodulation, and the method of demodulation of the second means of demodulation being a method of phase encoding demodulation.

20. The optical disk reproducer described in Claim 18, and further characterized by the decoding means including a number "n" of decoding keys, and selecting one of the decoding keys on the basis of a decoding key identification data reproduced from the main data in the optical disk.

21. The method of permitting the use of a program described in Claim 6, and characterized in that it comprises the further steps of:

connecting a first computer through a network to the second computer with a particular address;
sending to the second computer the first identification data for identifying the disk in the auxiliary data;
computing in the second computer the first identification data through a particular cipher operation, and sending the resultant (obtained) password to the first computer;
computing the password and the first identifica-

tion data in the decoding operation part of the first computer, and sending the resultant second decoding code to a cipher decoder; and

enabling an impermissible part of the main data in the optical disk to be used with the second decoding code by means of the cipher decoder.

22. A method of inspecting the illegal installation of a program, the method being characterized in that it comprises the steps of:

reproducing with a first computer an optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a reflection film is removed partially, so that auxiliary data are overwritten by a second method of modulation, which differs from the first method, the auxiliary data including a first identification data recorded therein for identifying individual optical disks, the main data including a first program, an installation program for installing the first program in the hard disk in the first computer, and a communication program recorded therein;
reproducing the first identification data from the auxiliary data;
installing the first program in the hard disk;
recording in the hard disk the first identification data or the first auxiliary identification data which is obtained from the first identification data through a predetermined computation; and
sending, when the installed first program starts or performs a particular operation, the first identification data or the first auxiliary identification data by means of the communication program to a second computer connected through a network to the first computer; or
checking through the network the second identification data which corresponds to the first identification data in the hard disk of the second computer or the second auxiliary identification data which is the second identification data computed through a particular operation; and
limiting the particular operation of the first program or adding a particular operation when the first and second identification data coincide or the first and second auxiliary identification data coincide.

23. An optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a reflection film is removed partially in the form of radially long bars from which the data cannot be read with the naked eye, so that auxiliary data are overwritten by a second method of modulation, which differs from the first method, at a lower recording density than the main data, the optical disk being characterized in:

that a first identification data for identifying individual optical disks is recorded in the auxiliary data;
that a first data is recorded in the main data in the first recording area of the optical disk, and
that a data associated with the first identification data is printed as a merchandise bar code which can be read by a merchandise bar code reader.

24. The optical disk described in Claim 23, and further characterized by the merchandise bar code being printed on the side other than the reproduction side of the optical disk.

25. A method of permission to use the program of a first data in an optical disk, the method being characterized in that it comprises the steps of:

reading a first identification data or a first auxiliary identification data with a merchandise bar code reader in a first computer from an optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is a predetermined area in the first recording area, where a reflection film is partially removed, so that auxiliary data are overwritten by a second method of modulation, which differs from the first method, the auxiliary data including the first identification data recorded therein for identifying individual optical disks, the main data in the first recording area of the optical disk including an impermissible part the use of which is not permitted, the optical disk having a bar code printed thereon from which the merchandise bar code reader can read the first identification data or the first auxiliary identification data associated with the first identification data;
sending the first identification data or the first auxiliary identification data through a network to a second computer;
computing with the second computer through a cipher operation on the basis of the first identification data to make a permission data which permits the use of an impermissible part;
sending the permission data to the first computer; and
printing the permission data on paper with a printing means by the first computer.

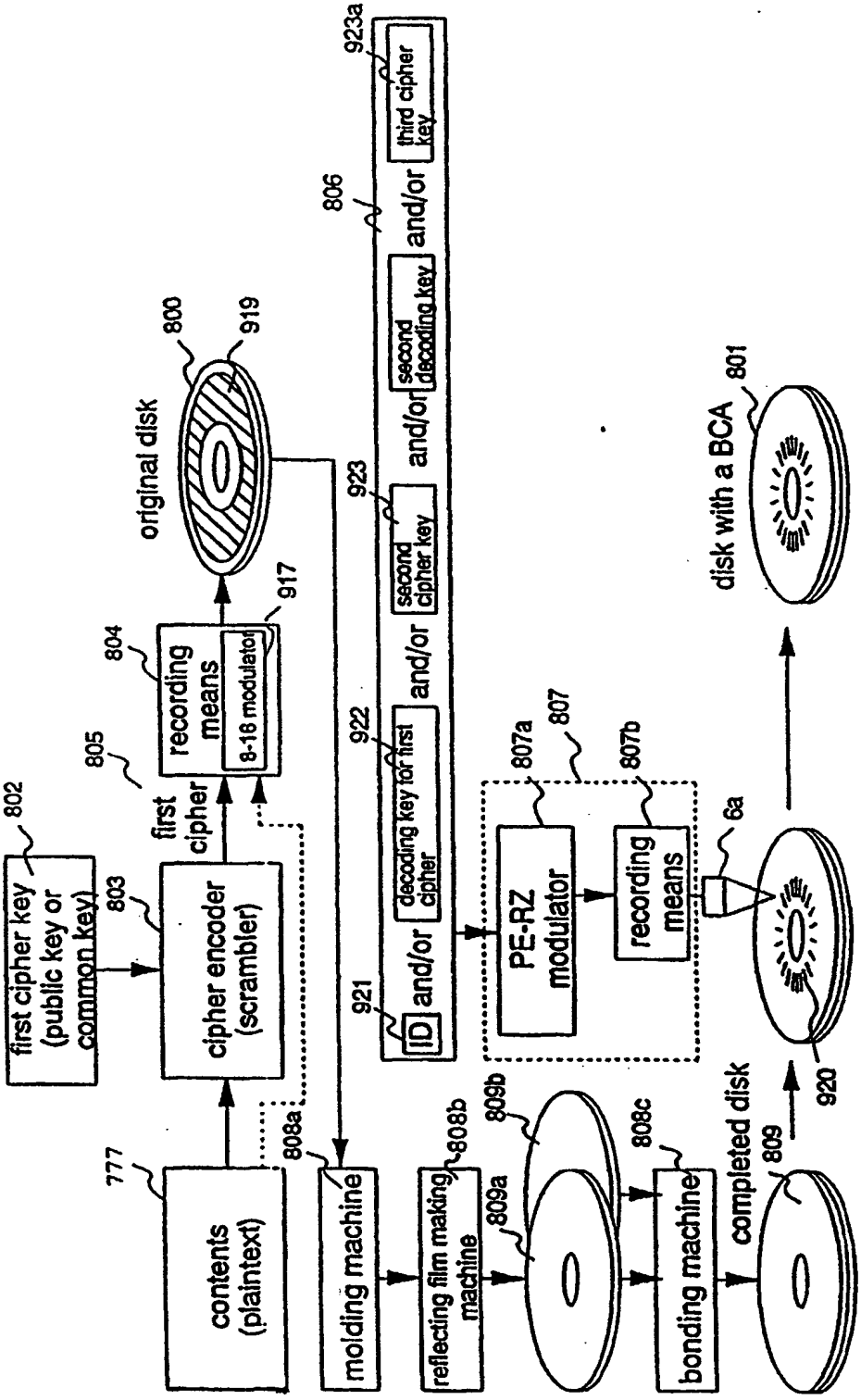
26. An optical disk including a first recording area, where main data are recorded in the form of pits, by a first method of modulation, and a second recording area which is the first predetermined area in the first recording area, where a plurality of radially long parts of a reflection film are removed partially, so that auxiliary data are overwritten over the pits in a low frequency band for frequency separation from the main data, the optical disk being characterized by:

    the auxiliary data including a first identification data recorded therein for identifying individual optical disks; and
    the main data including an impermissible part recorded therein which can be used with the first identification data and/or a specified password.

27. The optical disk described in Claim 26, and further characterized by being a read only type optical disk.

28. The optical disk described in Claim 26 or 27, and further characterized by the specified password being obtained through a specified operation with the first identification data.

Fig. 1


contents (plaintext)
777
first cipher key (public key or common key)
802
cipher encoder (scrambler)
803
first cipher
805
recording means
804
8-16 modulator
917
original disk
800
919
molding machine
808a
reflecting film making machine
808b
809a
809b
bonding machine
808c
completed disk
809
920
806
923
923a
ID and/or
921
decoding key for first cipher
and/or
922
second cipher key
and/or
second decoding key
and/or
third cipher key
PE-RZ modulator
807a
807
807b
recording means
6a
disk with a BCA
801

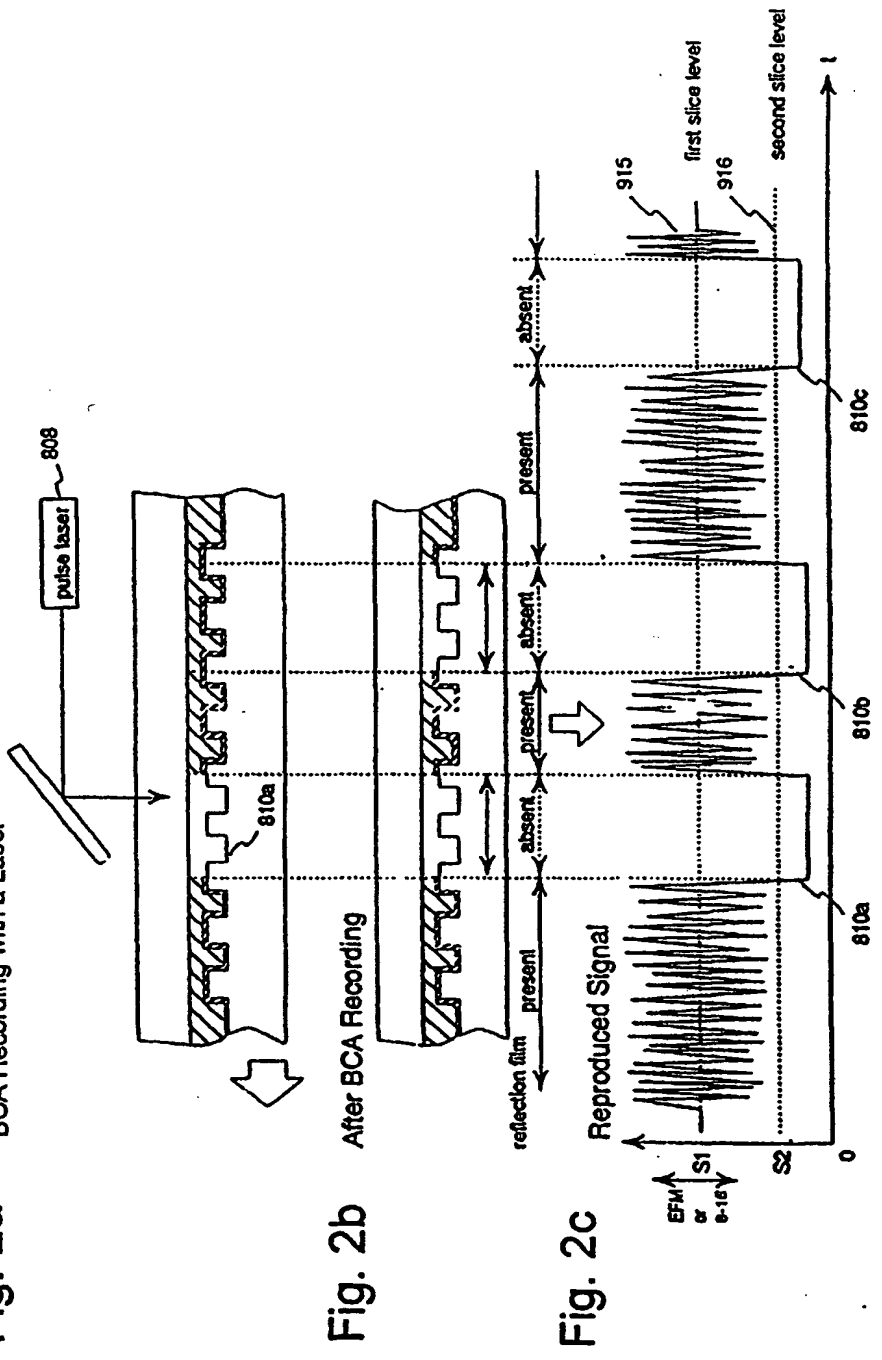



Fig. 2a

Fig. 2b

Fig. 2c

Fig. 3a Top Plan

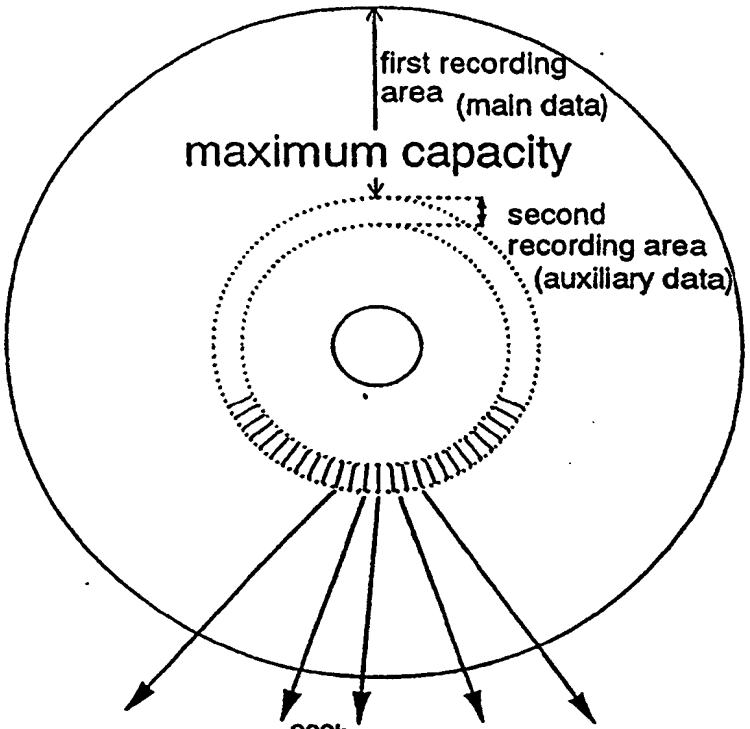



Fig. 3b Bar Code PE Modulation

Recorded Signal

Fig. 3c Recorded Signal

Fig. 3d Recorded Data

Reproduced Signal

Fig. 3e Reproduced Signal

Fig. 3f Filtered

Fig. 3g Reproduced Data

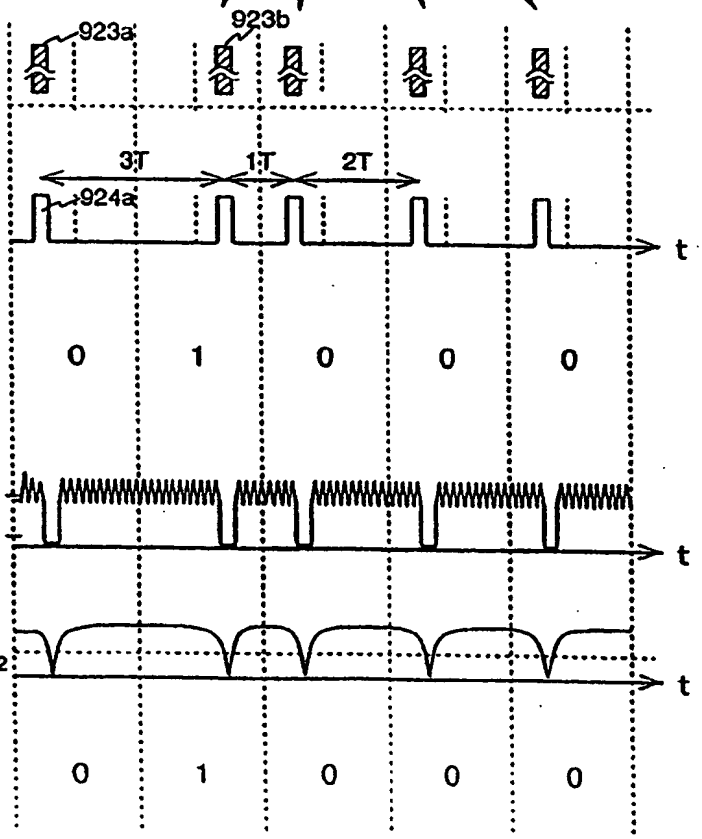


Fig. 4

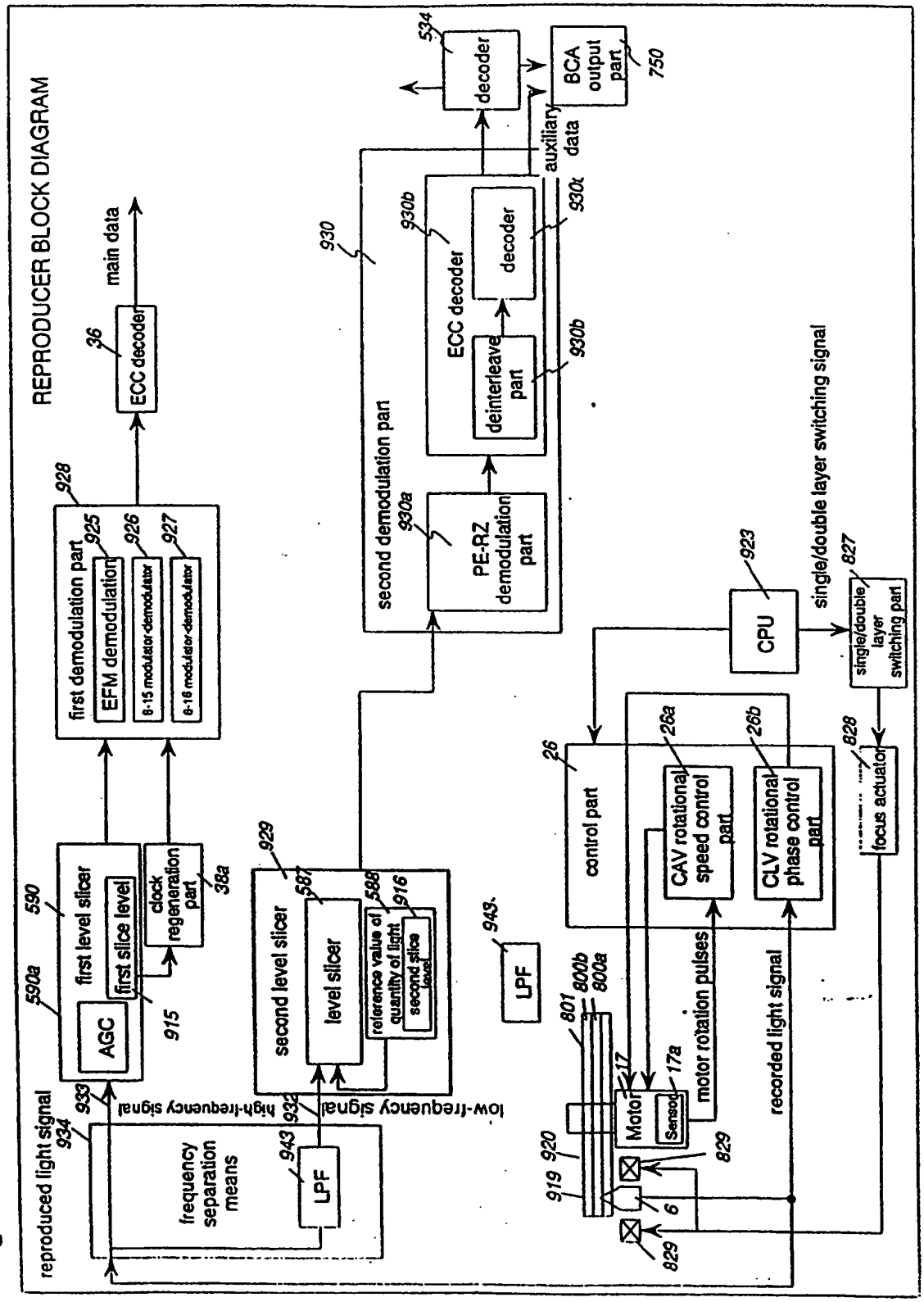

REPRODUCER BLOCK DIAGRAM
reproduced light signal
934
933
frequency separation means
943
LPF
high-frequency signal
932
low-frequency signal
590
590a
first level slicer
AGC
first slice level
915
clock regeneration part
38a
928
first demodulation part
925
EFM demodulation
926
8-15 modulator-demodulator
927
8-16 modulator-demodulator
36
ECC decoder
main data
929
second level slicer
587
level slicer
588
916
reference value of quantity of light
second slice level
943.
LPF
930
second demodulation part
930a
PE-RZ demodulation part
930b
ECC decoder
deinterleave part
decoder
930c
534
decoder
auxiliary data
BCA output part
750
923
CPU
single/double layer switching signal
827
single/double layer switching part
26
control part
26a
CAV rotational speed control part
26b
CLV rotational phase control part
828
focus actuator
801
800b
800a
17
Motor
17a
Sensor
motor rotation pulses
recorded light signal
919
920
829
6
829

Fig. 5a Waveform of Reproduced Signal Not Yet Filtered

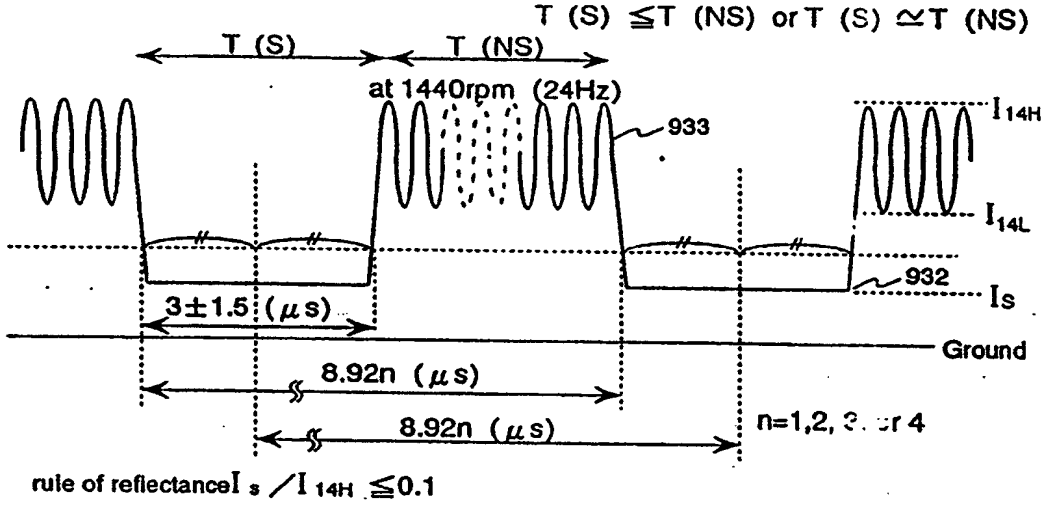



Fig. 5b Slit Dimension Accuracy (Precision) ( at r=22.2mm)

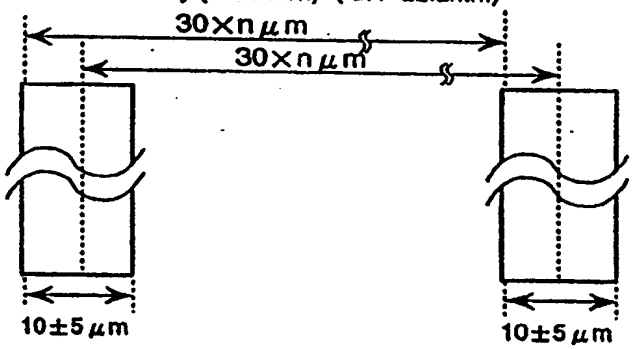
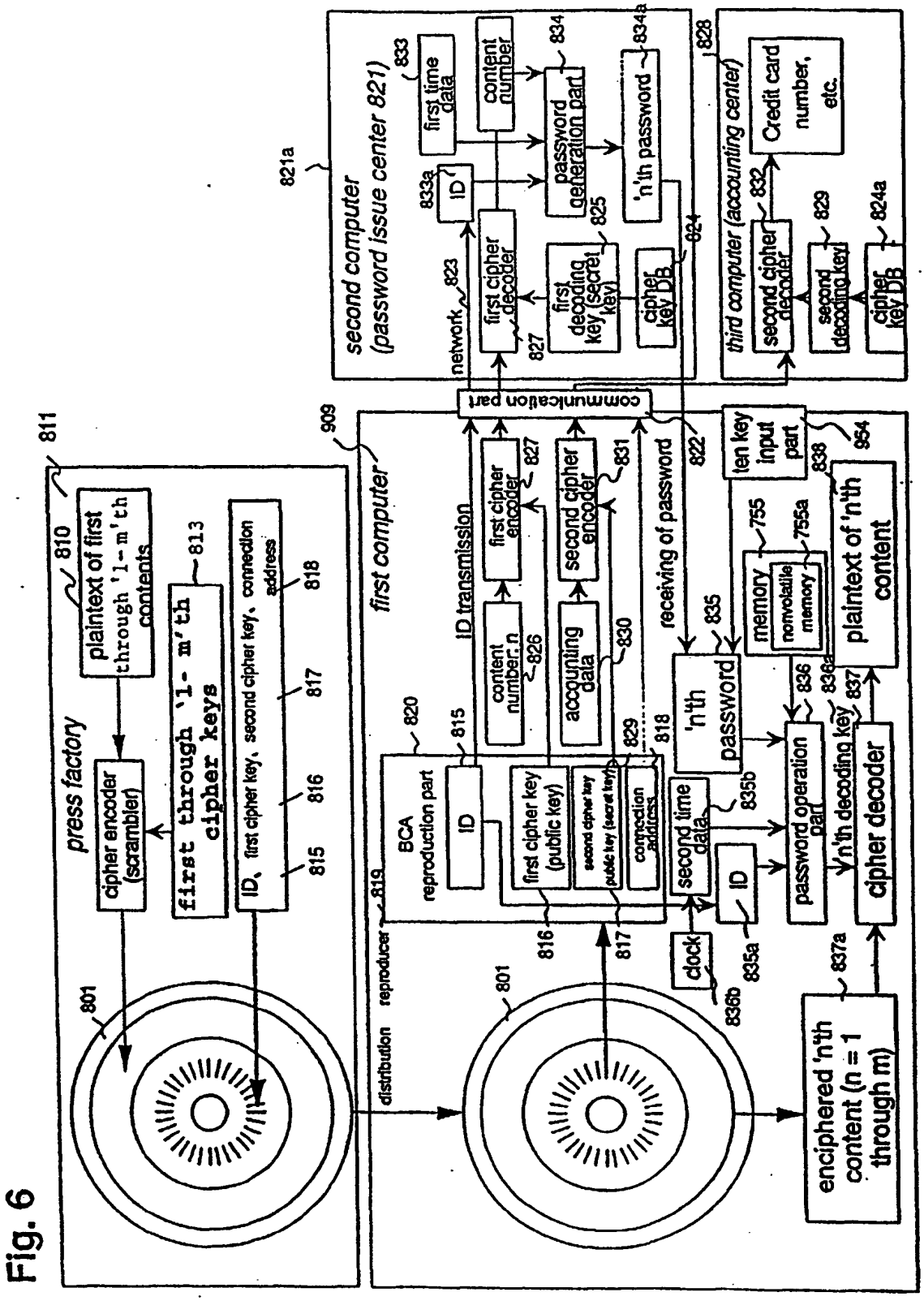


Fig. 6


press factory
811
plaintext of first through 'l-m'th contents
810
cipher encoder (scrambler)
first through 'l- m'th cipher keys
813
ID, first cipher key, second cipher key, connection address
818
817
816
815
801
distribution reproducer
819
first computer
909
BCA reproduction part
820
ID
815
first cipher key (public key)
second cipher key (secret key)
connection address
816
817
818
829
clock
836b
ID
835a
second time data
835b
'n'th password
835
password operation part
836
836a
n'th decoding key
837
837a
cipher decoder
enciphered 'n'th content (n = 1 through m)
ID transmission
content number, n
826
first cipher encoder
827
accounting data
830
second cipher encoder
831
receiving of password
822
communication part
ten key input part
838
954
memory
755
nonvolatile memory
755a
plaintext of 'n'th content
second computer (password issue center 821)
821a
network
823
first cipher decoder
827
ID
833a
first time data
833
content number
834
password generation part
825
first decoding key (secret key)
cipher key DB
824
'n'th password
834a
third computer (accounting center)
828
second cipher decoder
832
second decoding key
829
cipher key DB
824a
Credit card number, etc.

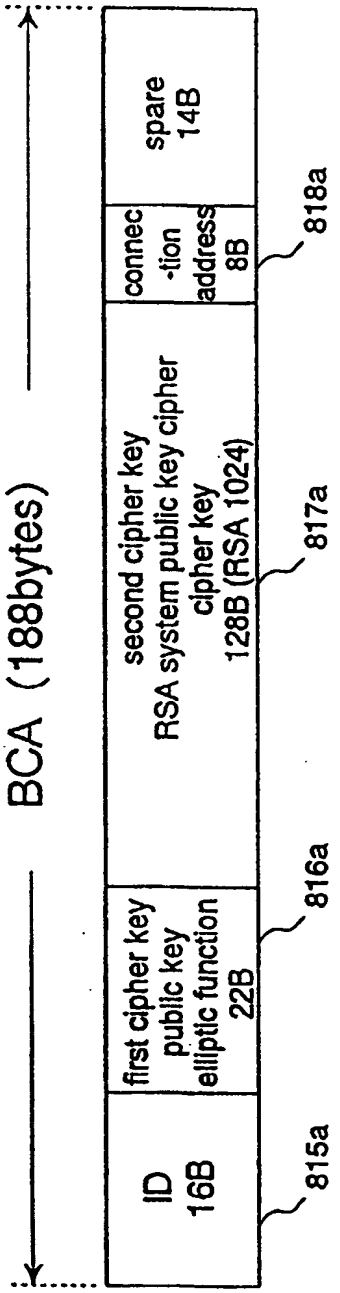



Fig. 7a

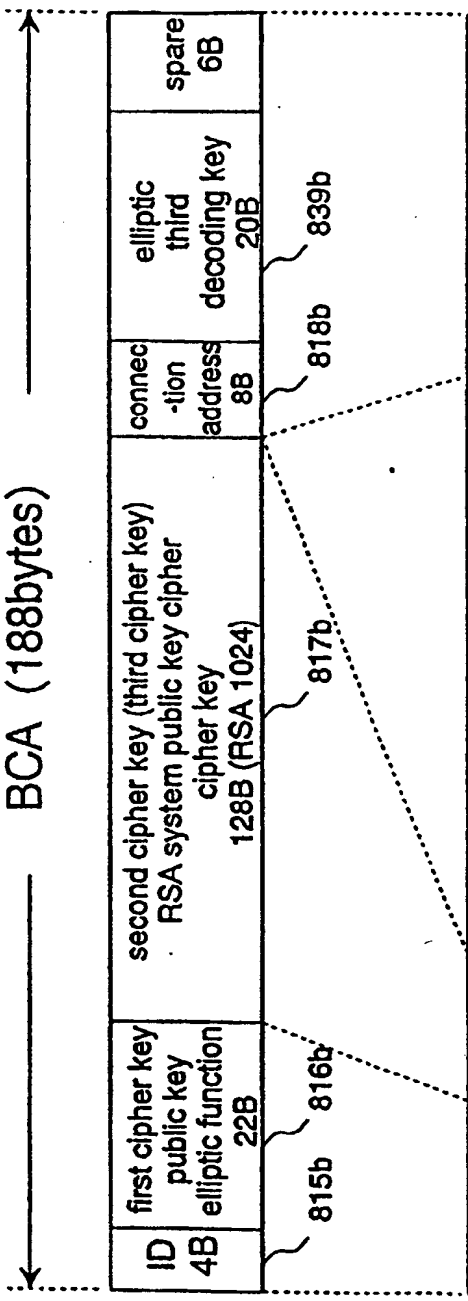



Fig. 7b

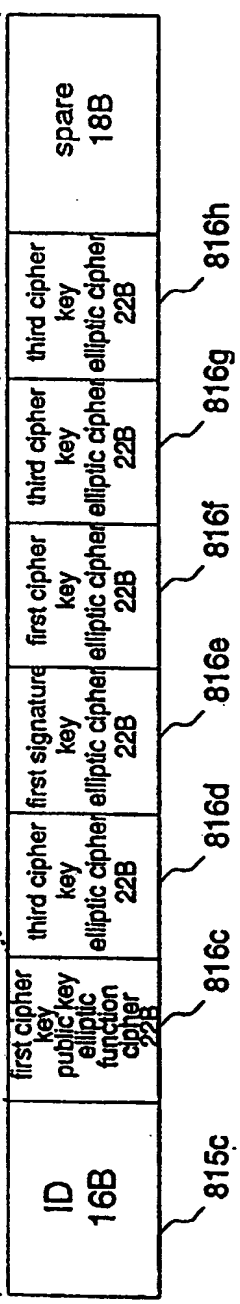



Fig. 7c

Fig. 8

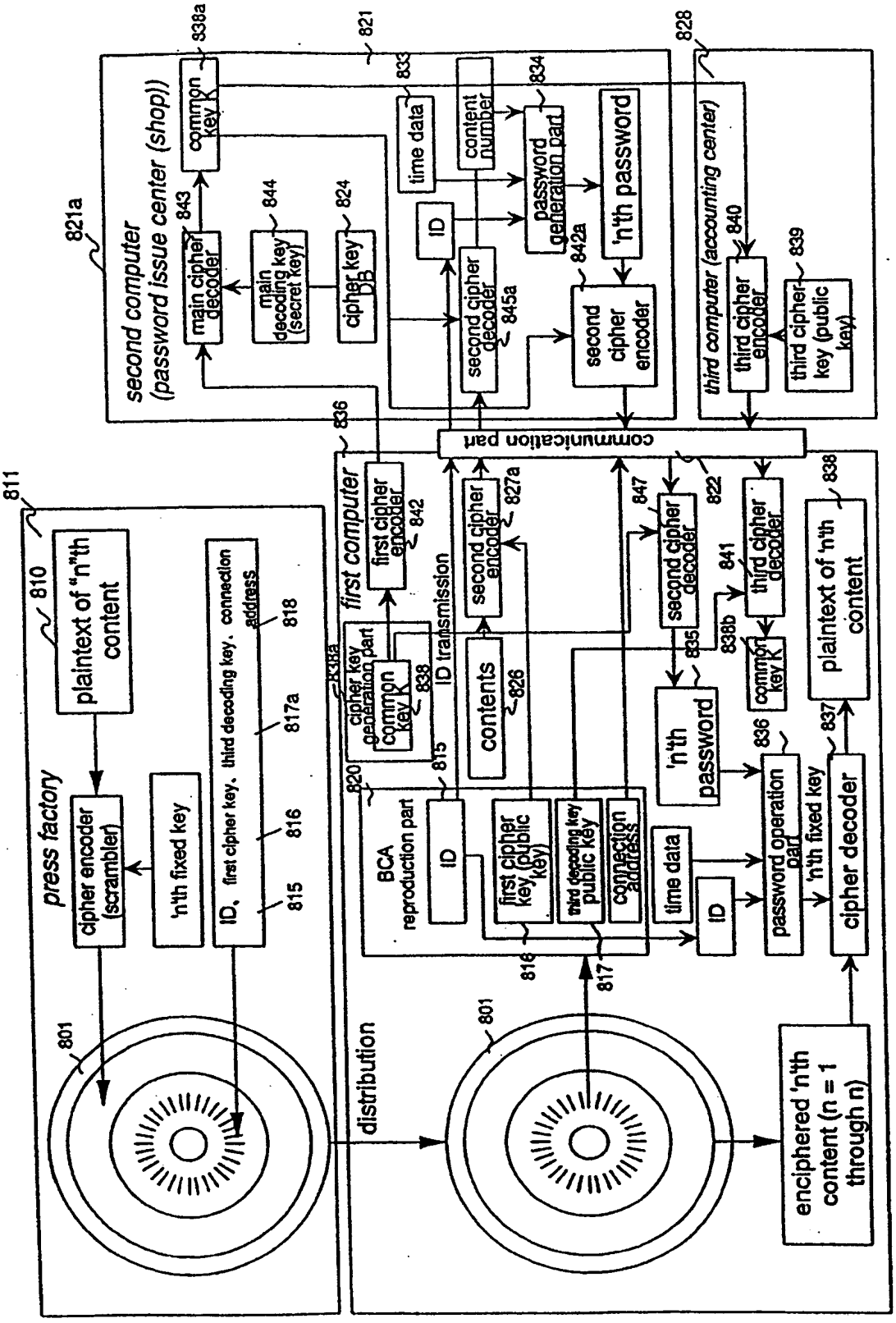

press factory
811
plaintext of "n"th content
810
cipher encoder (scrambler)
'n'th fixed key
ID, first cipher key, third decoding key, connection address
818
817a
816
815
801
distribution
first computer
821
cipher key generation part
838a
common key K
838
ID transmission
first cipher encoder
842
second cipher encoder
827a
contents
826
BCA reproduction part
820
ID
first cipher key (public key)
third decoding key public key
connection address
time data
'n'th password
password operation part
cipher decoder
'n'th fixed key
plaintext of 'n'th content
838
second cipher decoder
847
third cipher decoder
841
common key K
838b
835
822
836
837
enciphered 'n'th content (n = 1 through n)
communication part
second computer (password issue center (shop))
821a
common key K
838a
main cipher decoder
843
main decoding key (secret key)
844
cipher key DB
824
time data
833
content number
834
ID
password generation part
842a
'n'th password
second cipher decoder
845a
second cipher encoder
third computer (accounting center)
828
third cipher encoder
840
third cipher key (public key)
839

Fig. 9

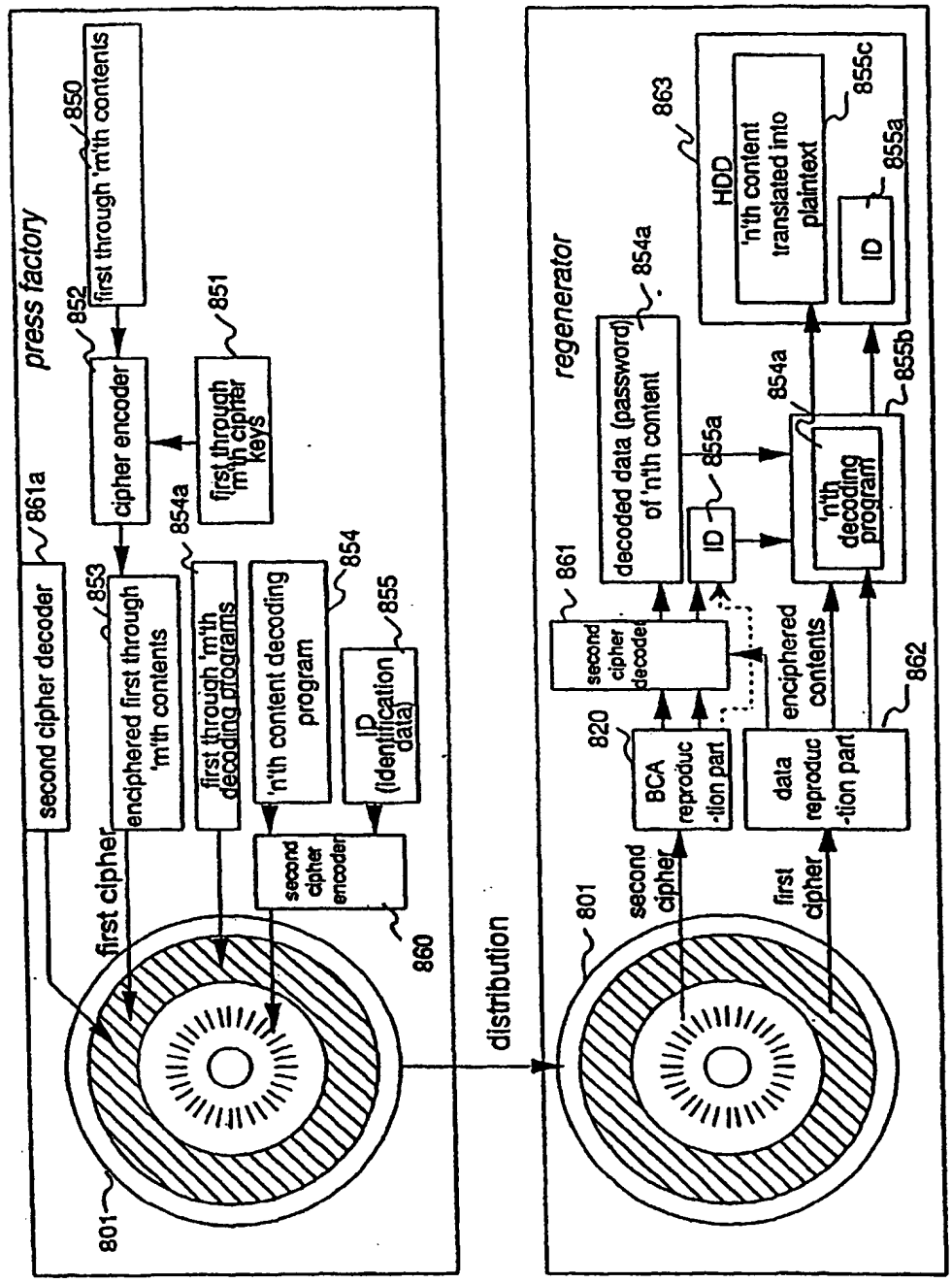

press factory
second cipher decoder
861a
first through 'm'th contents
850
852
cipher encoder
851
first through 'm'th cipher keys
854a
853
enciphered first through 'm'th contents
first through 'm'th decoding programs
'n'th content decoding program
854
855
ID (identification data)
second cipher encoder
860
first cipher
801
distribution
regenerator
863
HDD
'n'th content translated into plaintext
855c
ID
855a
854a
decoded data (password) of 'n'th content
855b
861
second cipher decoder
ID
855a
'n'th decoding program
854a
820
BCA reproduction part
data reproduction part
enciphered contents
862
second cipher
first cipher
801

Fig. 10

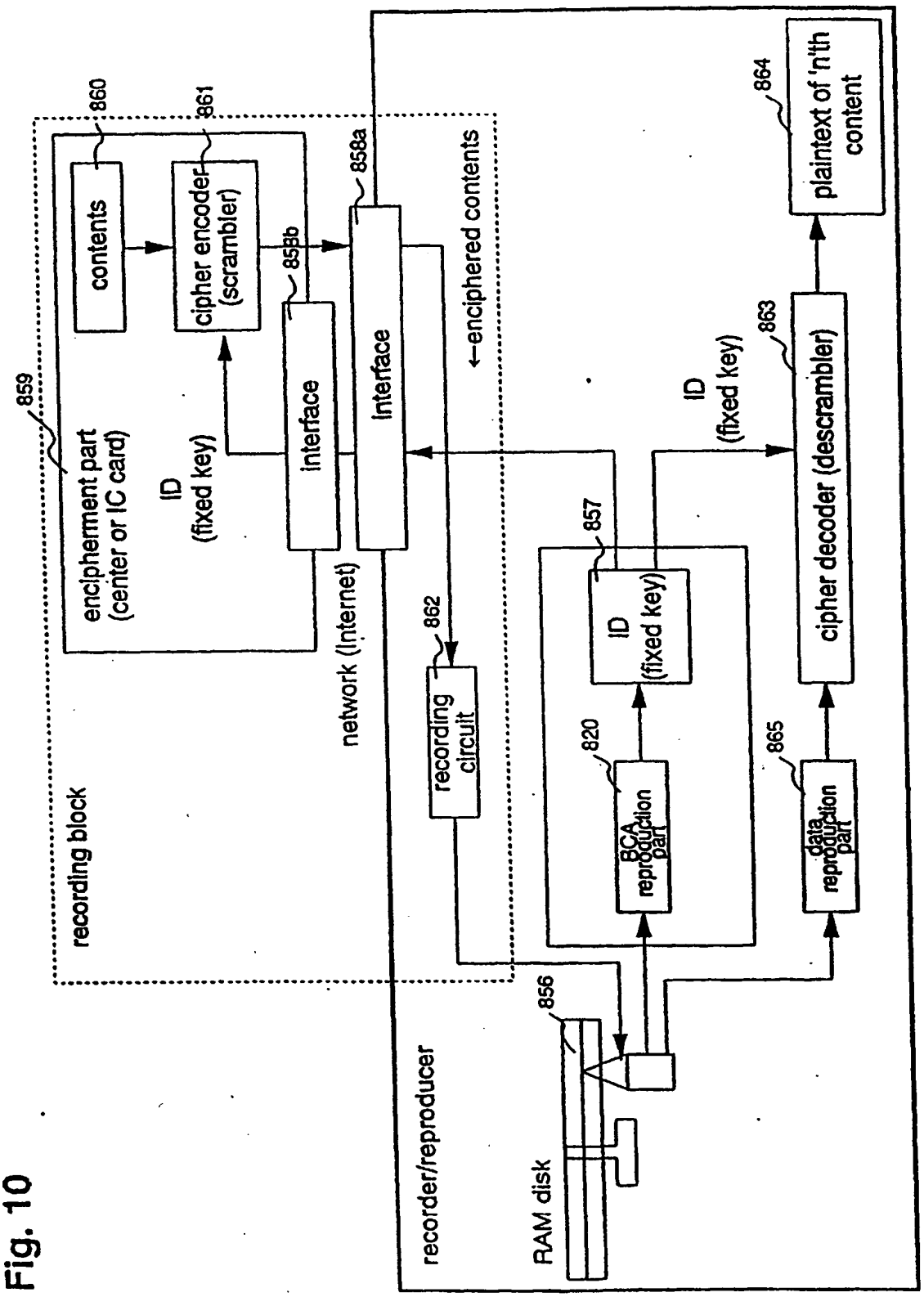

recorder/reproducer
recording block
encipherment part (center or IC card)
859
contents
860
cipher encoder (scrambler)
861
858b
interface
ID (fixed key)
858a
interface
network (Internet)
enciphered contents
recording circuit
862
856
RAM disk
857
ID (fixed key)
820
BCA reproduction part
865
data reproduction part
ID (fixed key)
863
cipher decoder (descrambler)
864
plaintext of 'n'th content

Fig. 11

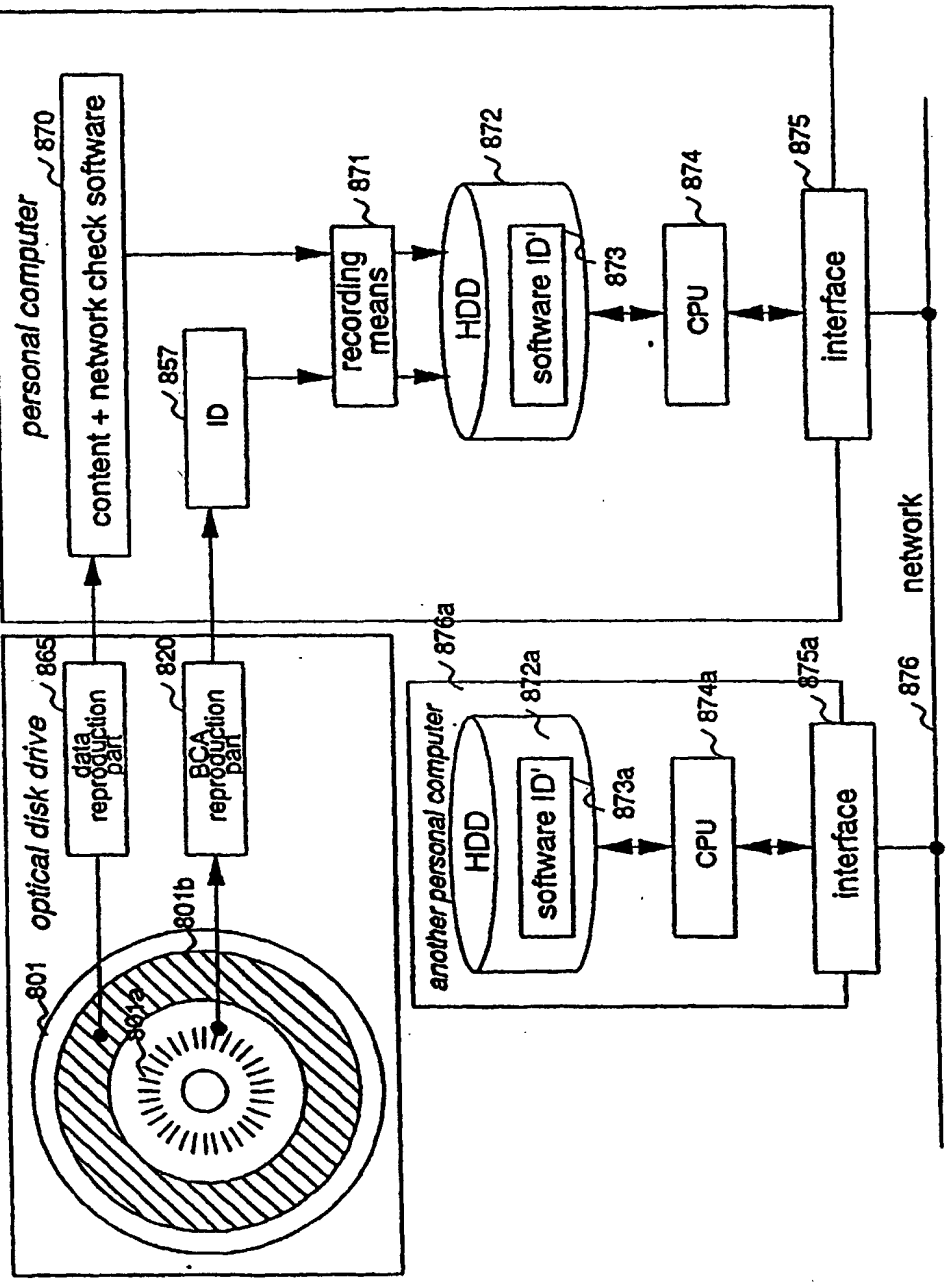
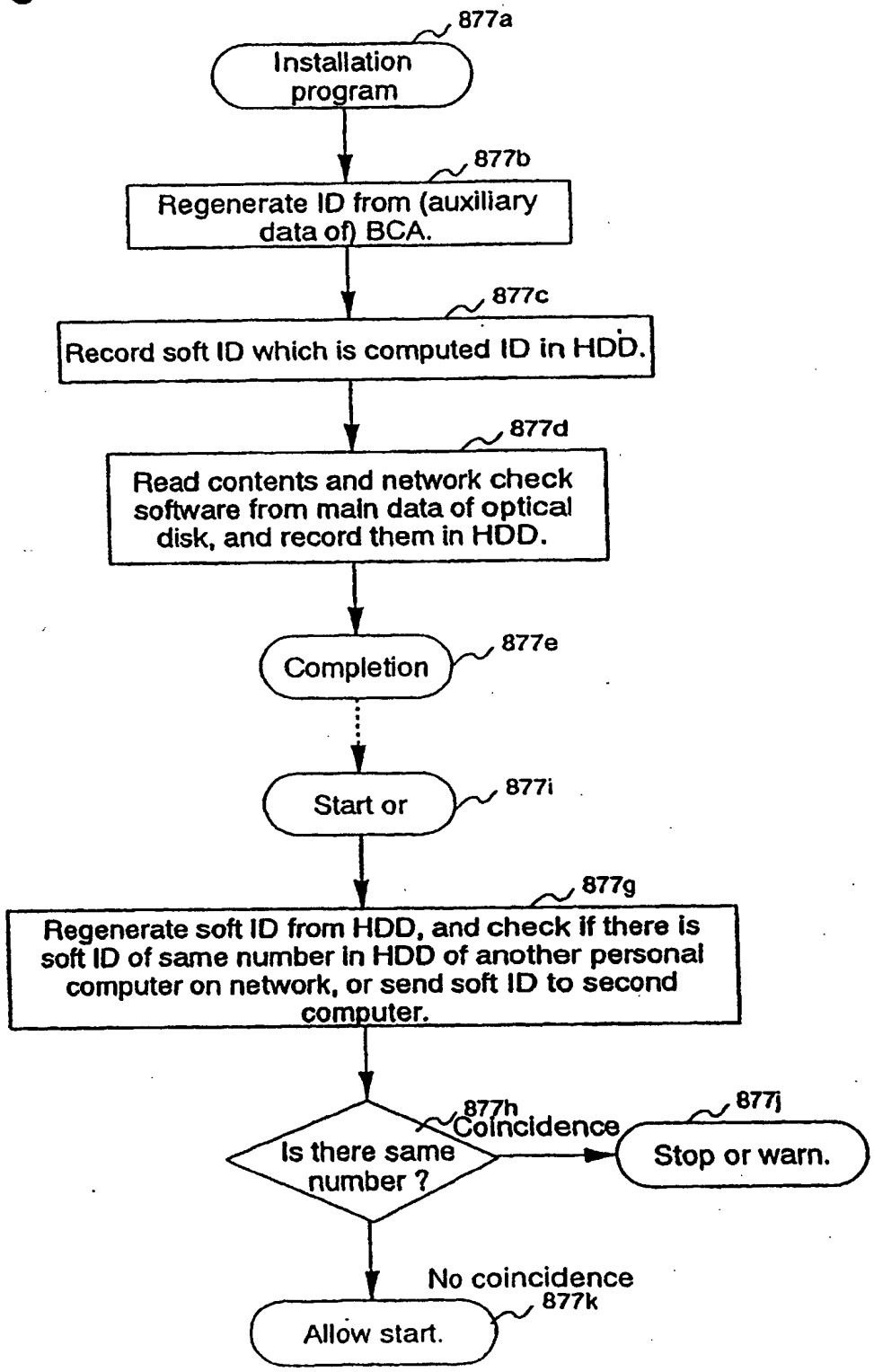

876
personal computer
870
content + network check software
recording means
871
HDD
872
software ID'
873
CPU
874
interface
875
857
ID
optical disk drive
865
data reproduction part
820
BCA reproduction part
801
801a
801b
876a
another personal computer
872a
873a
874a
875a
876
network

Fig. 12


877a
Installation program
877b
Regenerate ID from (auxiliary data of) BCA.
877c
Record soft ID which is computed ID in HDD.
877d
Read contents and network check software from main data of optical disk, and record them in HDD.
Completion
877e
Start or
877i
877g
Regenerate soft ID from HDD, and check if there is soft ID of same number in HDD of another personal computer on network, or send soft ID to second computer.
877h
Is there same number ?
Coincidence
877j
Stop or warn.
No coincidence
877k
Allow start.

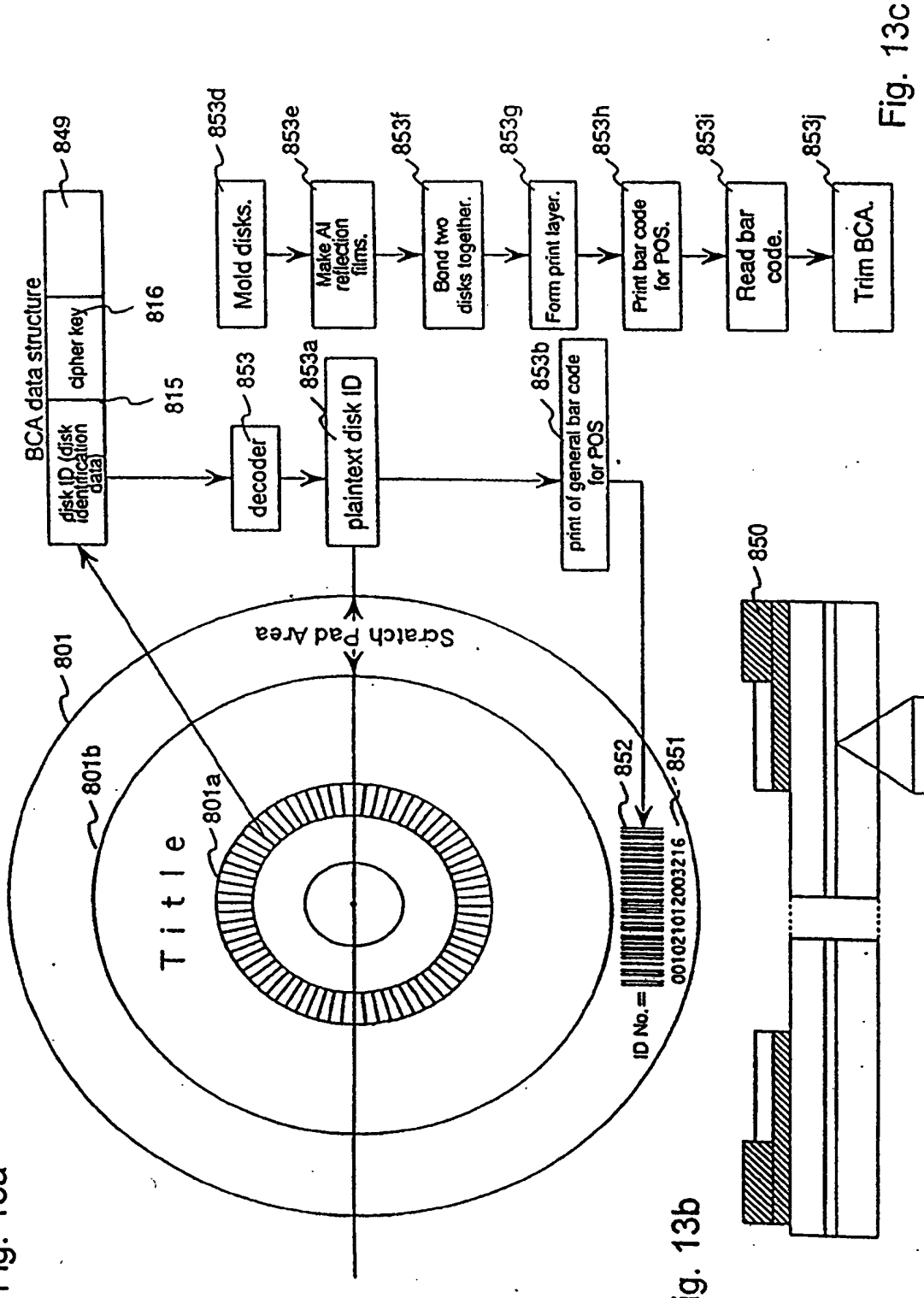



Fig. 13a

Fig. 13b

Fig. 13c

Fig. 14

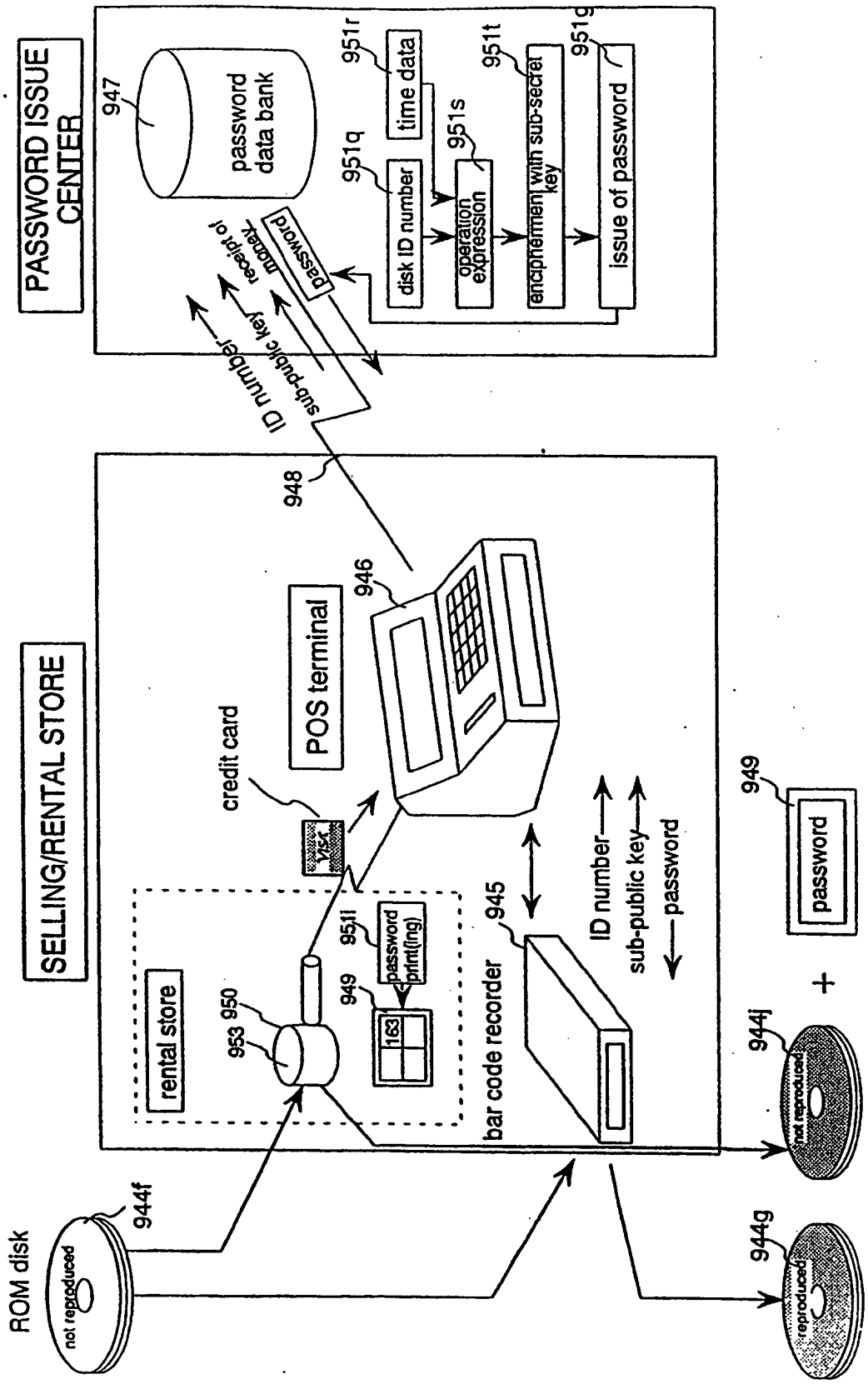

PASSWORD ISSUE CENTER
947
password data bank
951r
time data
951t
951q
disk ID number
951s
operation expression
encipherment with sub-secret key
951g
issue of password
password
receipt of money
sub-public key
ID number
948
SELLING/RENTAL STORE
946
POS terminal
credit card
rental store
951i
password print(ing)
949
953 950
945
bar code recorder
ID number
sub-public key
password
949
password
944j
not reproduced
+
944f
ROM disk
not reproduced
944g
reproduced

Fig. 15

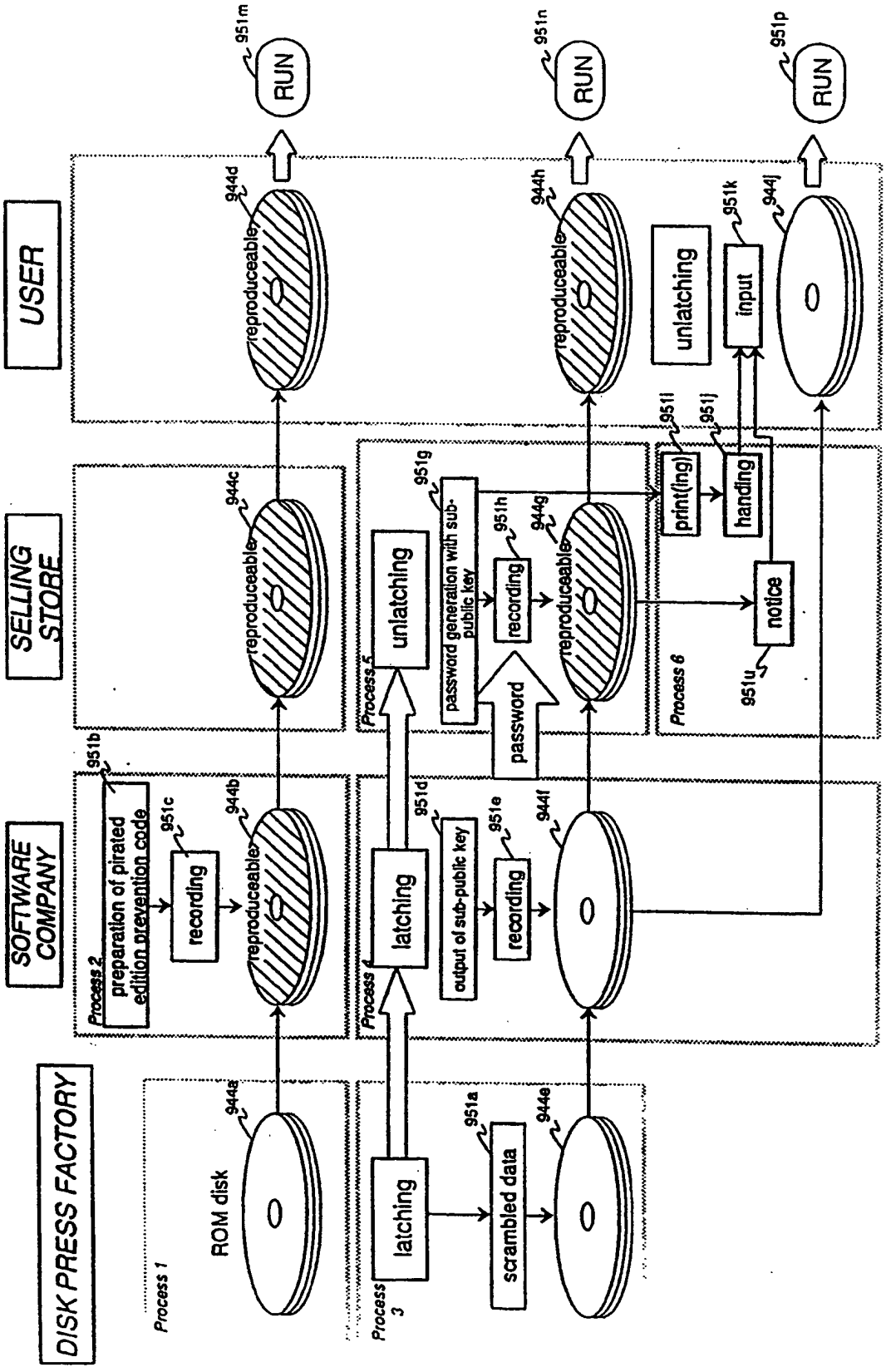

DISK PRESS FACTORY
SOFTWARE COMPANY
SELLING STORE
USER
Process 1
ROM disk
944a
Process 2
preparation of pirated edition prevention code
951b
recording
951c
reproduceable
944b
Process 3
latching
951d
scrambled data
951a
944e
Process 4
latching
output of sub-public key
951e
recording
944f
Process 5
unlatching
password generation with sub-public key
951g
recording
951h
password
944g
reproduceable
944c
reproduceable
944d
RUN
951m
Process 6
print(ing)
951i
handing
951j
notice
951u
unlatching
input
951k
944h
reproduceable
RUN
951n
944j
RUN
951p

Fig. 16

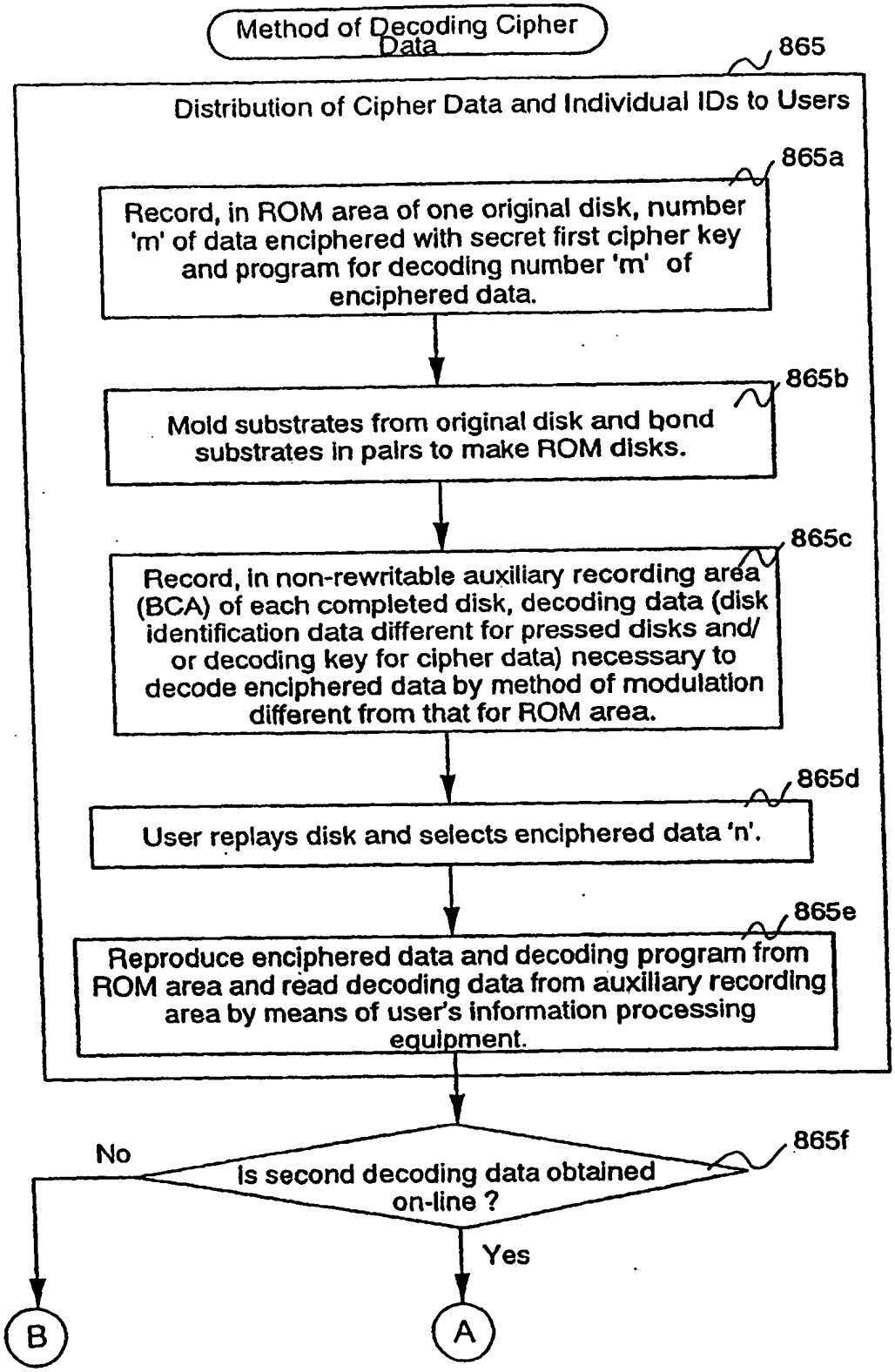

Method of Decoding Cipher Data
865
Distribution of Cipher Data and Individual IDs to Users
865a
Record, in ROM area of one original disk, number 'm' of data enciphered with secret first cipher key and program for decoding number 'm' of enciphered data.
865b
Mold substrates from original disk and bond substrates in pairs to make ROM disks.
865c
Record, in non-rewritable auxiliary recording area (BCA) of each completed disk, decoding data (disk identification data different for pressed disks and/or decoding key for cipher data) necessary to decode enciphered data by method of modulation different from that for ROM area.
865d
User replays disk and selects enciphered data 'n'.
865e
Reproduce enciphered data and decoding program from ROM area and read decoding data from auxiliary recording area by means of user's information processing equipment.
865f
No
Is second decoding data obtained on-line ?
Yes
B
A

Fig. 17

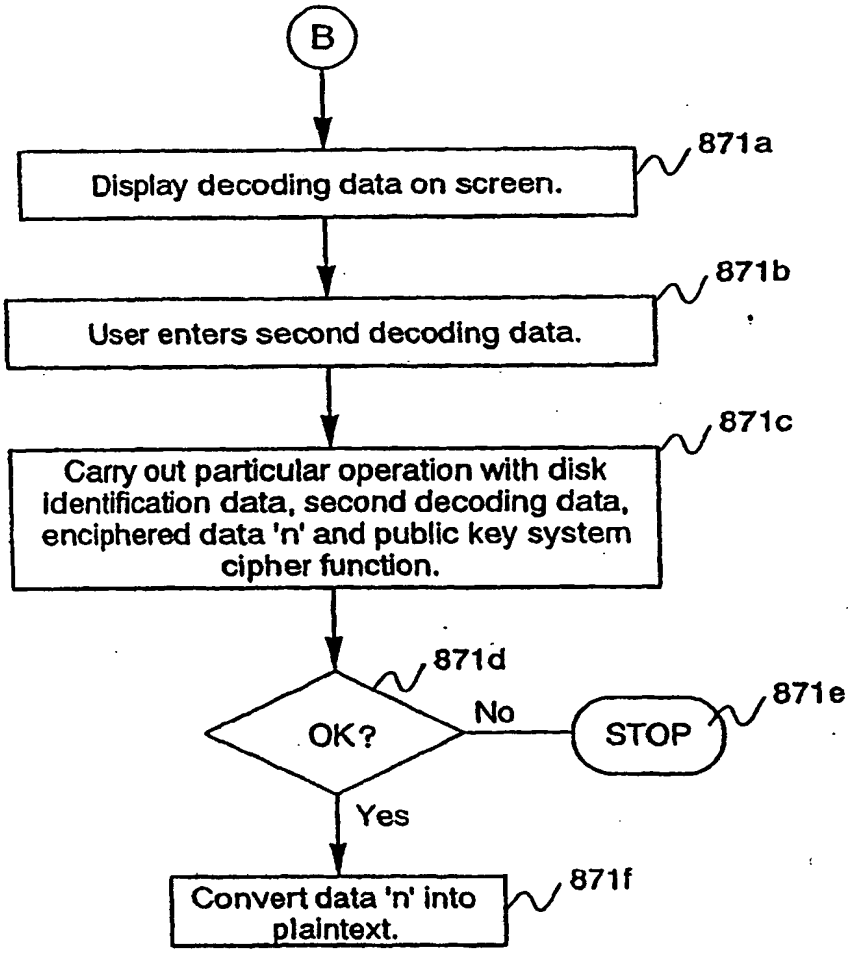

B
Display decoding data on screen.
871a
User enters second decoding data.
871b
Carry out particular operation with disk identification data, second decoding data, enciphered data 'n' and public key system cipher function.
871c
871d
OK?
No
STOP
871e
Yes
Convert data 'n' into plaintext.
871f

Fig. 18

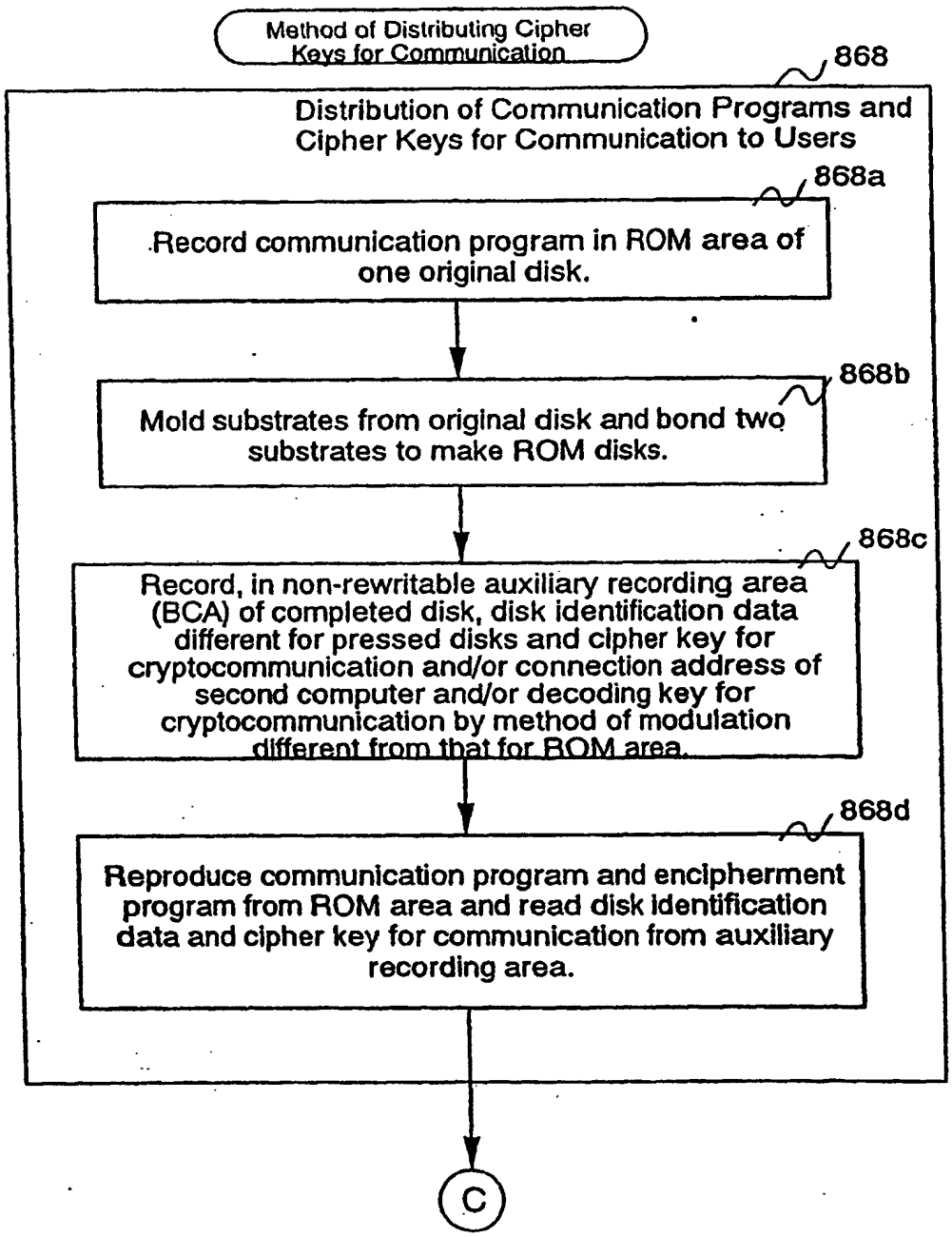

Method of Distributing Cipher Keys for Communication
868
Distribution of Communication Programs and Cipher Keys for Communication to Users
868a
Record communication program in ROM area of one original disk.
868b
Mold substrates from original disk and bond two substrates to make ROM disks.
868c
Record, in non-rewritable auxiliary recording area (BCA) of completed disk, disk identification data different for pressed disks and cipher key for cryptocommunication and/or connection address of second computer and/or decoding key for cryptocommunication by method of modulation different from that for ROM area.
868d
Reproduce communication program and encipherment program from ROM area and read disk identification data and cipher key for communication from auxiliary recording area.
C

Fig. 19

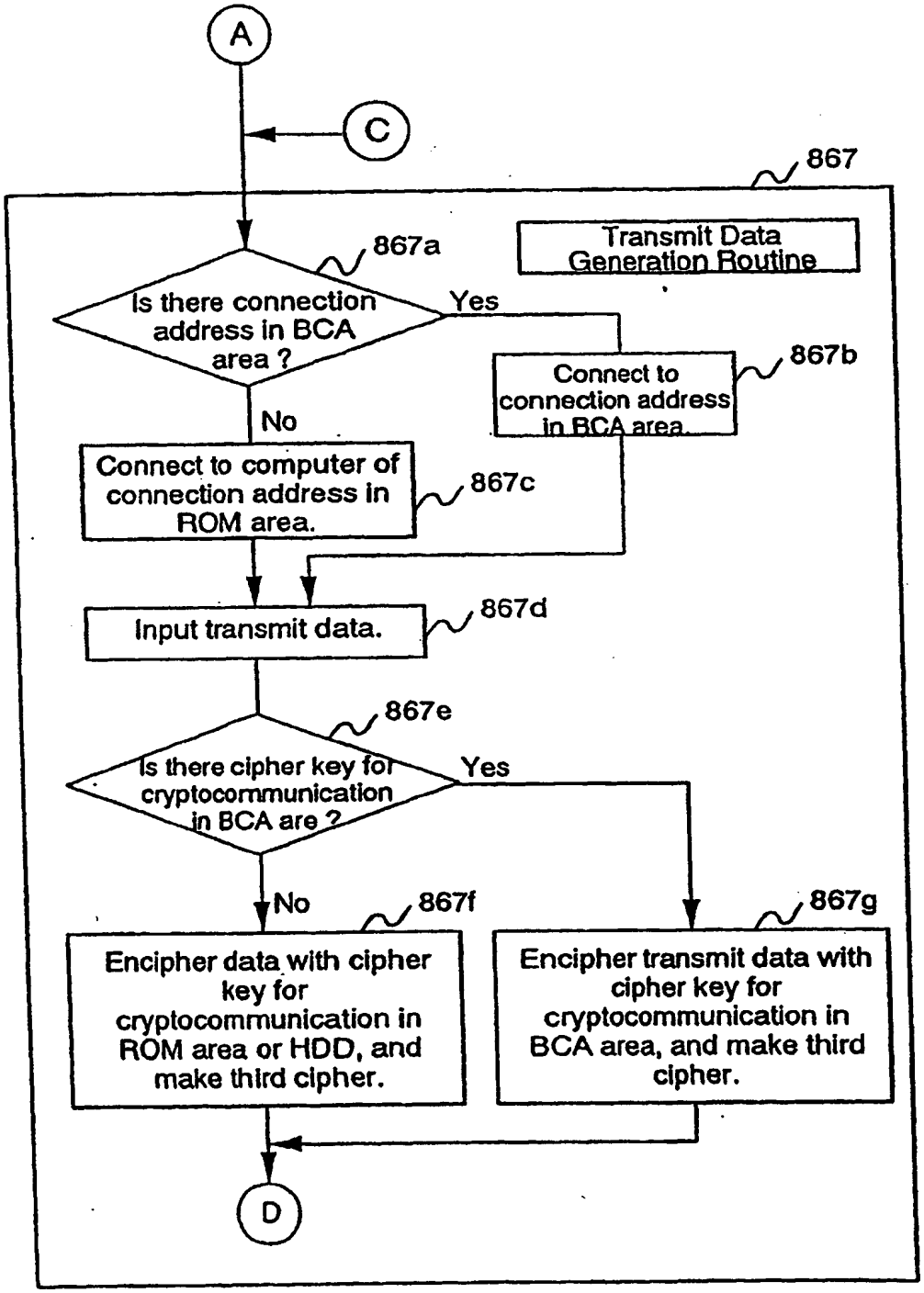

A
C
867
Transmit Data Generation Routine
867a
Is there connection address in BCA area ?
Yes
No
867b
Connect to connection address in BCA area.
Connect to computer of connection address in ROM area.
867c
Input transmit data.
867d
867e
Is there cipher key for cryptocommunication in BCA are ?
Yes
No
867f
867g
Encipher data with cipher key for cryptocommunication in ROM area or HDD, and make third cipher.
Encipher transmit data with cipher key for cryptocommunication in BCA area, and make third cipher.
D

Fig. 20

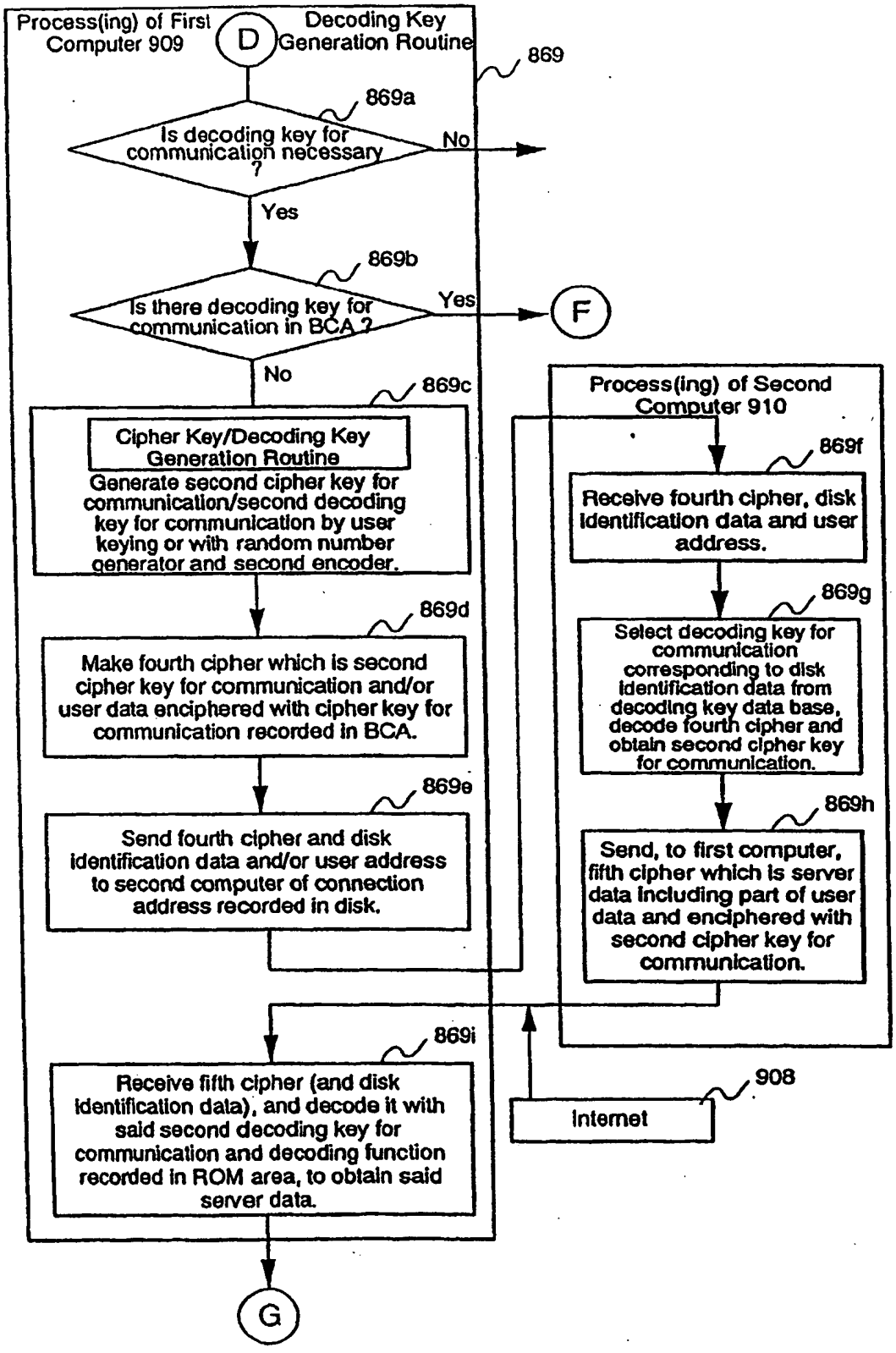

Process(ing) of First Computer 909
D
Decoding Key Generation Routine
869
869a
Is decoding key for communication necessary ?
No
Yes
869b
Is there decoding key for communication in BCA ?
Yes
F
No
869c
Cipher Key/Decoding Key Generation Routine
Generate second cipher key for communication/second decoding key for communication by user keying or with random number generator and second encoder.
869d
Make fourth cipher which is second cipher key for communication and/or user data enciphered with cipher key for communication recorded in BCA.
869e
Send fourth cipher and disk identification data and/or user address to second computer of connection address recorded in disk.
869i
Receive fifth cipher (and disk identification data), and decode it with said second decoding key for communication and decoding function recorded in ROM area, to obtain said server data.
G
Process(ing) of Second Computer 910
869f
Receive fourth cipher, disk identification data and user address.
869g
Select decoding key for communication corresponding to disk identification data from decoding key data base, decode fourth cipher and obtain second cipher key for communication.
869h
Send, to first computer, fifth cipher which is server data including part of user data and enciphered with second cipher key for communication.
908
Internet

Fig. 21

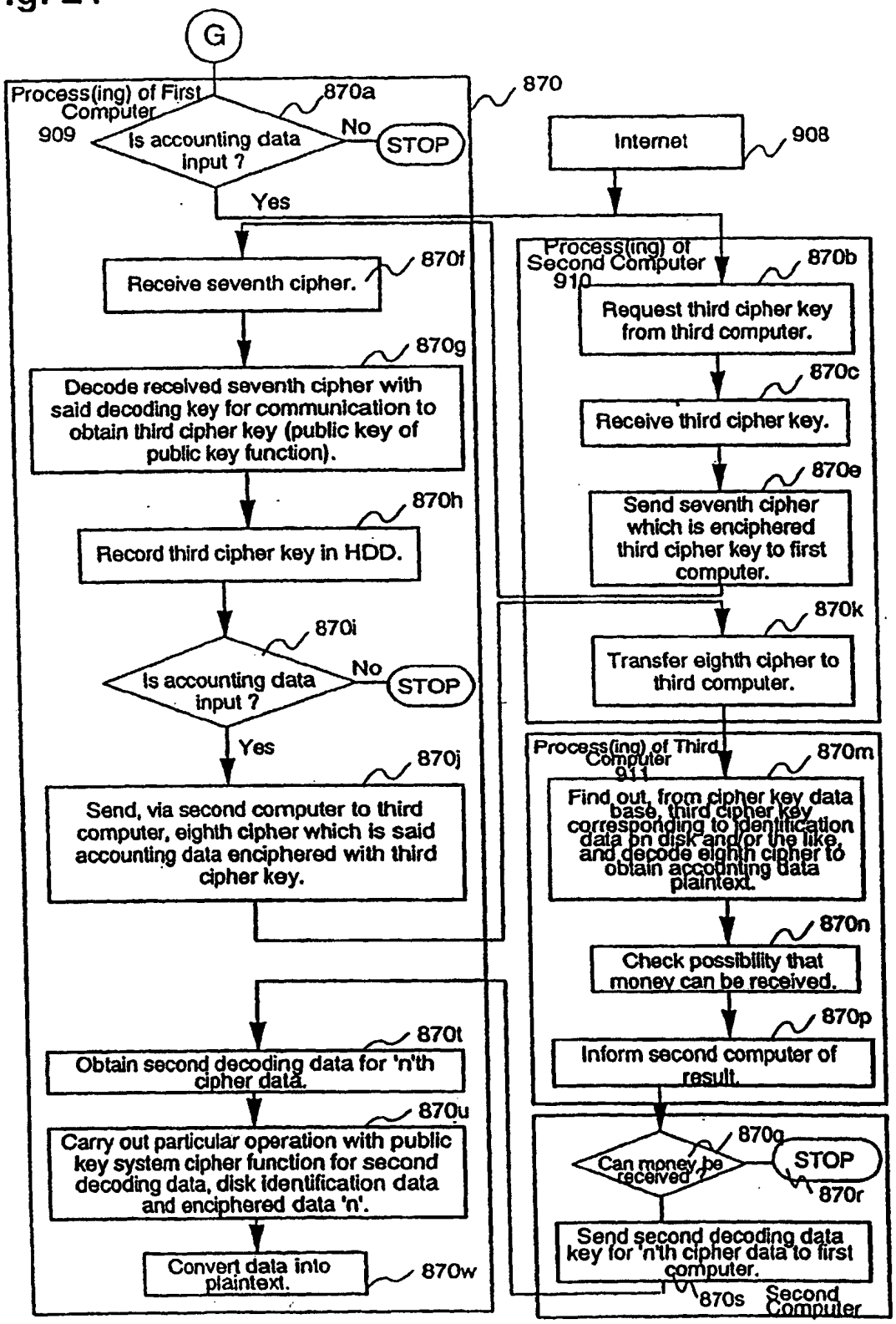

G
Process(ing) of First Computer
909
870a
Is accounting data input ?
No
STOP
Yes
870
Internet
908
Receive seventh cipher.
870f
Decode received seventh cipher with said decoding key for communication to obtain third cipher key (public key of public key function).
870g
Record third cipher key in HDD.
870h
Is accounting data input ?
870i
No
STOP
Yes
Send, via second computer to third computer, eighth cipher which is said accounting data enciphered with third cipher key.
870j
Obtain second decoding data for 'n'th cipher data.
870t
Carry out particular operation with public key system cipher function for second decoding data, disk identification data and enciphered data 'n'.
870u
Convert data into plaintext.
870w
Process(ing) of Second Computer
910
Request third cipher key from third computer.
870b
Receive third cipher key.
870c
Send seventh cipher which is enciphered third cipher key to first computer.
870e
Transfer eighth cipher to third computer.
870k
Process(ing) of Third Computer
911
Find out, from cipher key data base, third cipher key corresponding to identification data on disk and/or the like, and decode eighth cipher to obtain accounting data plaintext.
870m
Check possibility that money can be received.
870n
Inform second computer of result.
870p
Can money be received ?
870q
STOP
870r
Send second decoding data key for 'n'th cipher data to first computer.
870s
Second Computer

Fig. 22

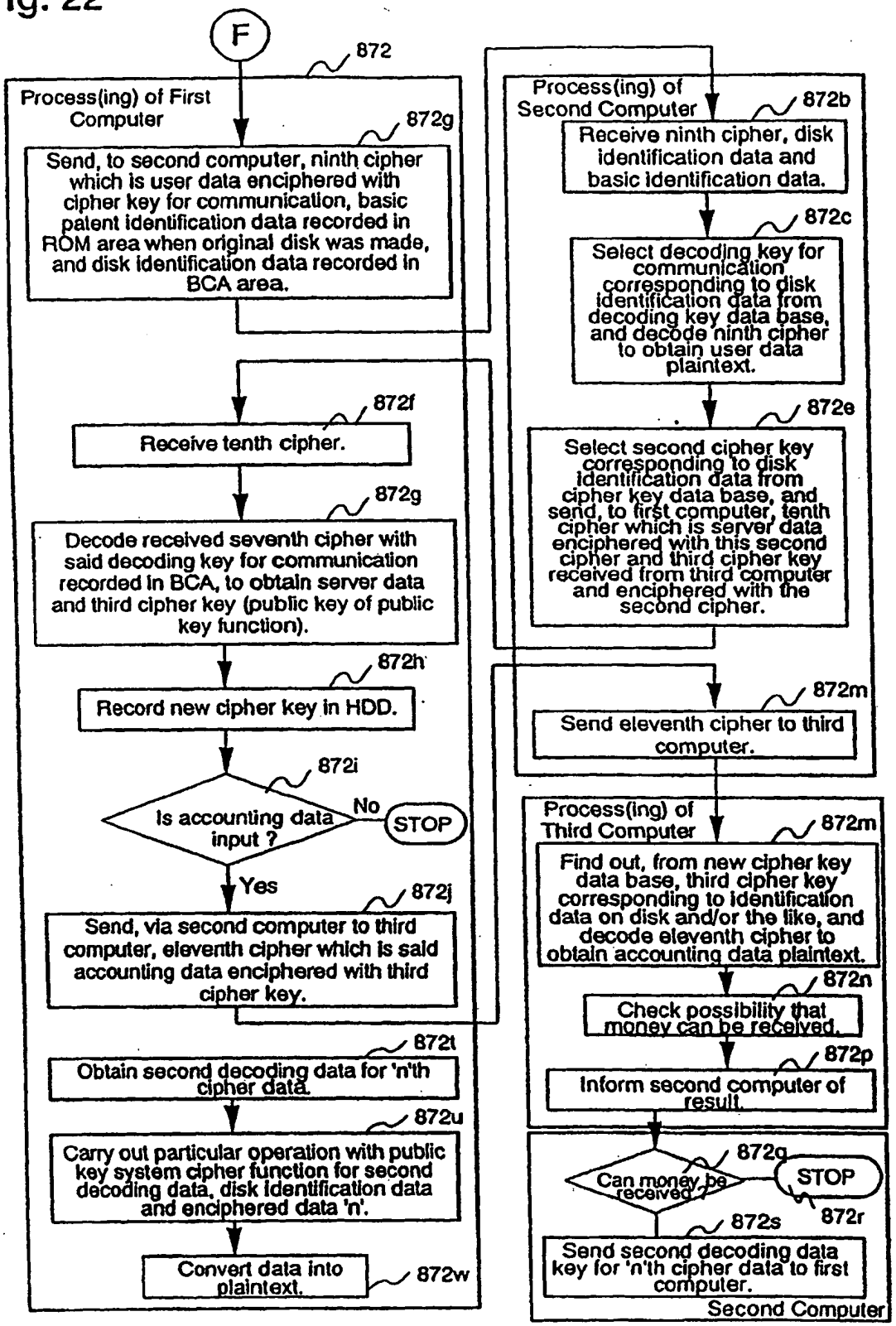

F
872
Process(ing) of First Computer
872g
Send, to second computer, ninth cipher which is user data enciphered with cipher key for communication, basic patent identification data recorded in ROM area when original disk was made, and disk identification data recorded in BCA area.
872f
Receive tenth cipher.
872g
Decode received seventh cipher with said decoding key for communication recorded in BCA, to obtain server data and third cipher key (public key of public key function).
872h
Record new cipher key in HDD.
872i
Is accounting data input ?
No
STOP
Yes
872j
Send, via second computer to third computer, eleventh cipher which is said accounting data enciphered with third cipher key.
872t
Obtain second decoding data for 'n'th cipher data.
872u
Carry out particular operation with public key system cipher function for second decoding data, disk identification data and enciphered data 'n'.
Convert data into plaintext.
872w
Process(ing) of Second Computer
872b
Receive ninth cipher, disk identification data and basic identification data.
872c
Select decoding key for communication corresponding to disk identification data from decoding key data base, and decode ninth cipher to obtain user data plaintext.
872e
Select second cipher key corresponding to disk identification data from cipher key data base, and send, to first computer, tenth cipher which is server data enciphered with this second cipher and third cipher key received from third computer and enciphered with the second cipher.
872m
Send eleventh cipher to third computer.
Process(ing) of Third Computer
872m
Find out, from new cipher key data base, third cipher key corresponding to identification data on disk and/or the like, and decode eleventh cipher to obtain accounting data plaintext.
872n
Check possibility that money can be received.
872p
Inform second computer of result.
872q
Can money be received ?
STOP
872r
872s
Send second decoding data key for 'n'th cipher data to first computer.
Second Computer

Fig. 23

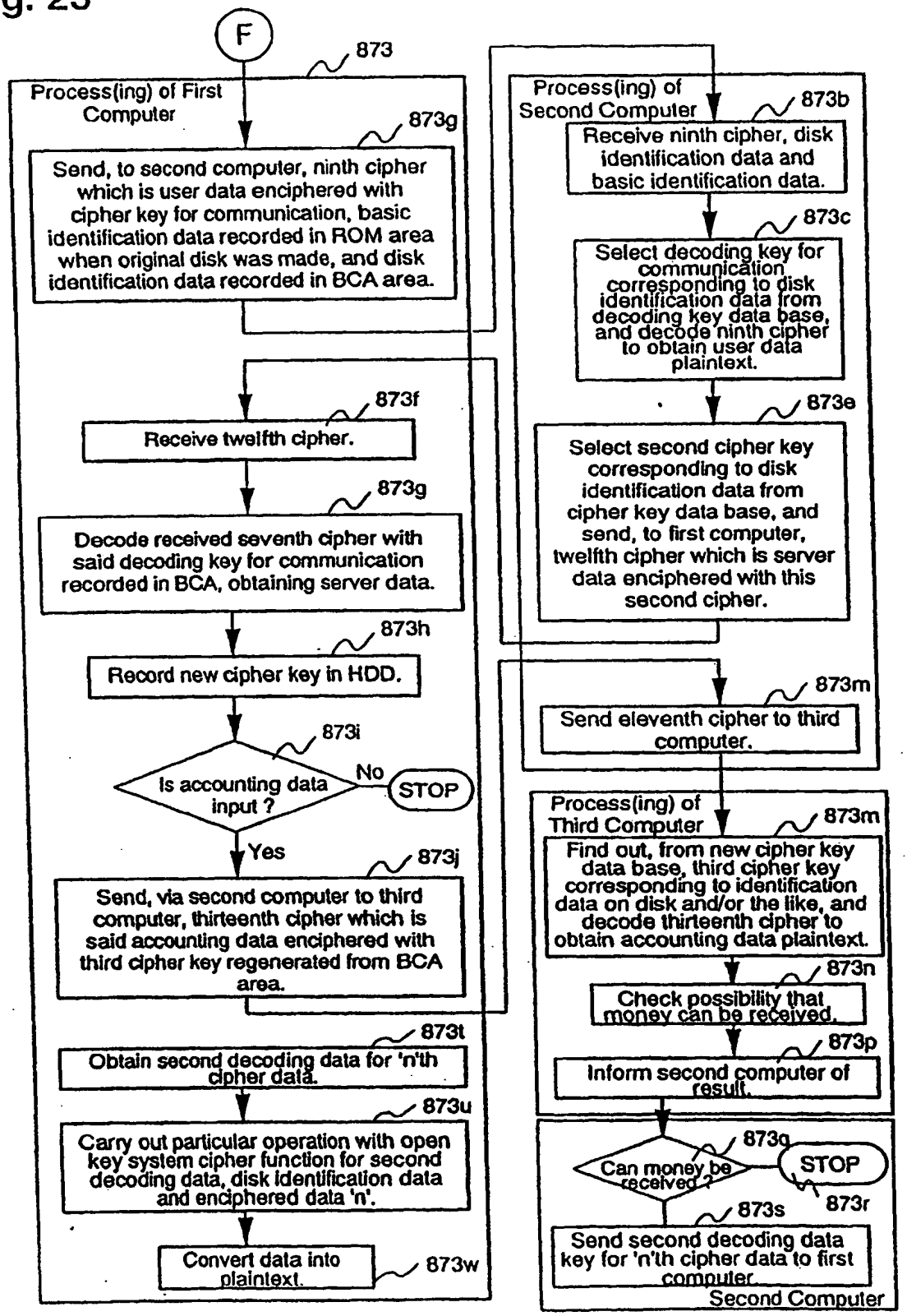
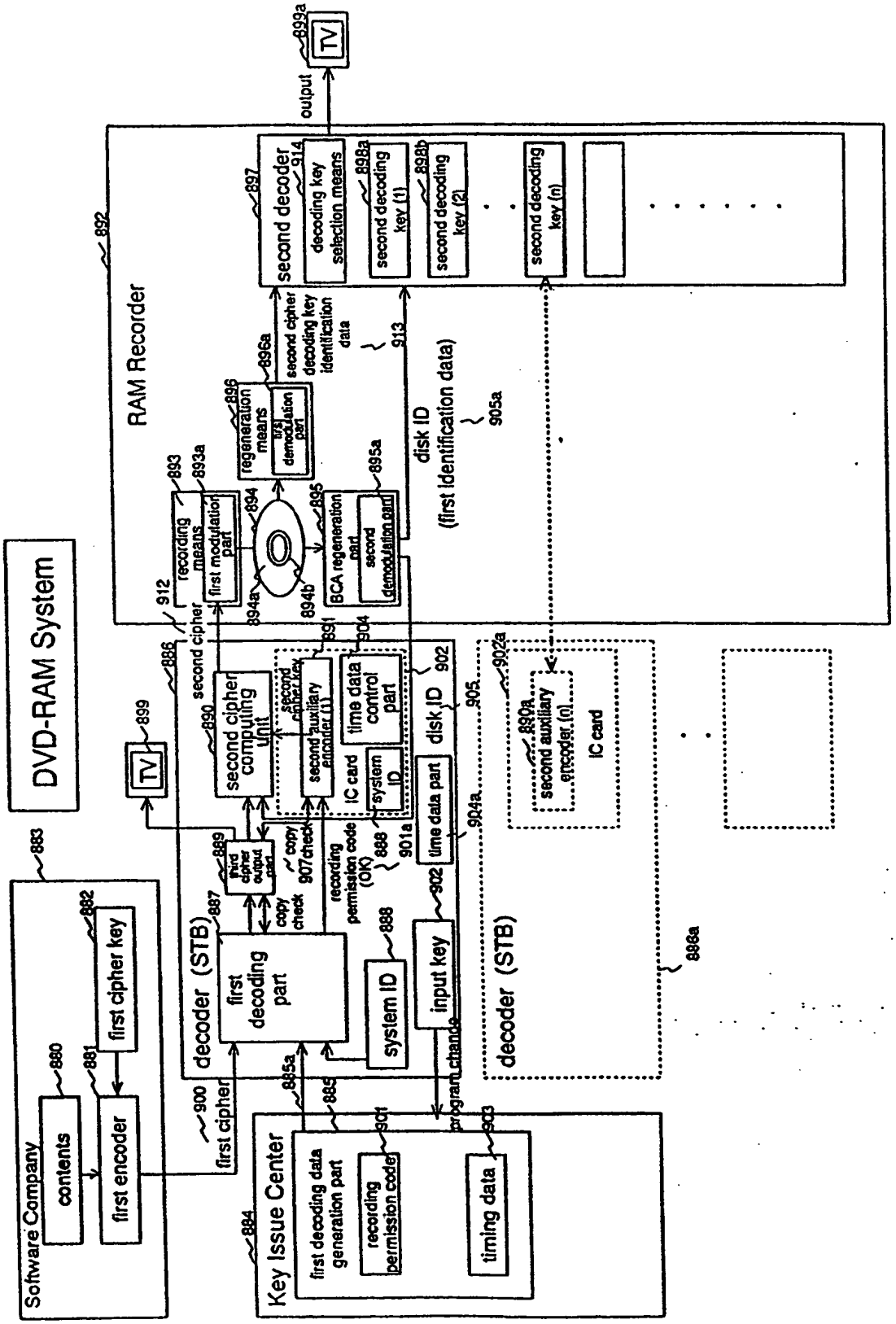

F
873
Process(ing) of First Computer
873g
Send, to second computer, ninth cipher which is user data enciphered with cipher key for communication, basic identification data recorded in ROM area when original disk was made, and disk identification data recorded in BCA area.
873f
Receive twelfth cipher.
873g
Decode received seventh cipher with said decoding key for communication recorded in BCA, obtaining server data.
873h
Record new cipher key in HDD.
873i
Is accounting data input ?
No
STOP
Yes
873j
Send, via second computer to third computer, thirteenth cipher which is said accounting data enciphered with third cipher key regenerated from BCA area.
873t
Obtain second decoding data for 'n'th cipher data.
873u
Carry out particular operation with open key system cipher function for second decoding data, disk identification data and enciphered data 'n'.
Convert data into plaintext.
873w
Process(ing) of Second Computer
873b
Receive ninth cipher, disk identification data and basic identification data.
873c
Select decoding key for communication corresponding to disk identification data from decoding key data base, and decode ninth cipher to obtain user data plaintext.
873e
Select second cipher key corresponding to disk identification data from cipher key data base, and send, to first computer, twelfth cipher which is server data enciphered with this second cipher.
873m
Send eleventh cipher to third computer.
Process(ing) of Third Computer
873m
Find out, from new cipher key data base, third cipher key corresponding to identification data on disk and/or the like, and decode thirteenth cipher to obtain accounting data plaintext.
873n
Check possibility that money can be received.
873p
Inform second computer of result.
873q
Can money be received ?
STOP
873r
873s
Send second decoding data key for 'n'th cipher data to first computer.
Second Computer

Fig. 24


DVD-RAM System
Software Company
contents
first encoder
first cipher key
first cipher
Key Issue Center
first decoding data generation part
recording permission code
timing data
program change
decoder (STB)
first decoding part
system ID
input key
third cipher output part
copy check
recording permission code (OK)
IC card
system ID
second auxiliary encoder (1)
second cipher computing unit
second cipher
time data control part
time data part
disk ID
TV
RAM Recorder
recording means
first modulation part
BCA regeneration part
second demodulation part
regeneration means
first demodulation part
second cipher decoding key identification data
second decoder
decoding key selection means
second decoding key (1)
second decoding key (2)
second decoding key (n)
output
disk ID
(first identification data)
second auxiliary encoder (n)
IC card
decoder (STB)

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP96/02924

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl$^6$ G11B7/00, G11B20/10, G06F12/14, G06F9/06
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
Int. Cl$^6$ G11B7/00, G11B20/10, G06F12/14, G06F9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1955 - 1996
Kokai Jitsuyo Shinan Koho 1971 - 1996
Toroku Jitsuyo Shinan Koho 1994 - 1996

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | JP, 58-21143, A (Sony Corp.), December 8, 1983 (08. 12. 83)(Family: none) | 1 - 28 |
| A | JP, 61-71487, A (Hoya Corp.), April 12, 1986 (12. 04. 86)(Family: none) | 1 - 28 |
| A | JP, 2-293930, A (Victor Co. of Japan, Ltd.), December 5, 1990 (05. 12. 90) & US, 5379433, A | 1 - 28 |
| A | SHINGAKU GIHO Vol. 94, No. 240, Technical Paper of the Inst. of Electronics, Information and Communication Engineers of Japan, Information Security, ISEC94-13-22, September 21, 1994 Makoto Yoshioka, Ryota Akiyama "Trend of Superdistribution Technology" pp. 67-74 | 6 - 28 |
| A | SHINGAKU GIHO Vol. 94, No. 240, Technical Paper of the Inst. of Electronics, Information and Communication Engineers of Japan, Information Security, ISEC94-13-22, September 21, 1994 | 6 - 28 |

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| December 5, 1996 (05. 12. 96) | December 17, 1996 (17. 12. 96) |
| Name and mailing address of the ISA/ Japanese Patent Office<br>Facsimile No. | Authorized officer<br>Telephone No. |

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP96/02924

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| | Yoshimichi Nakazawa "Software Distribution Technology with CD-ROM" p. 41-46 | |

Form PCT/ISA/210 (continuation of second sheet) (July 1992)